

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-149504

(43)Date of publication of application : 02.06.1999

(51)Int.Cl.

G06F 17/60  
G06F 15/00

(21)Application number : 09-315473

(22)Date of filing : 17.11.1997

(71)Applicant : HITACHI LTD

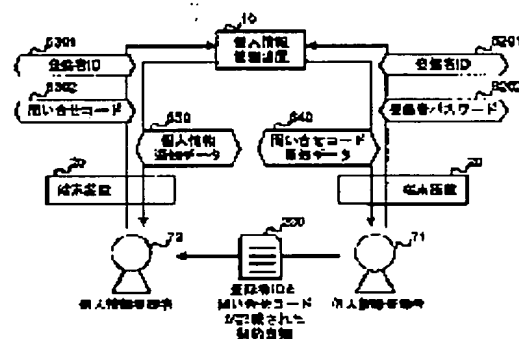
(72)Inventor : TAKAHASHI HIDEO  
NITTA ATSUSHI  
TASAKA MITSUNOBU  
TAKEDA AKIRA

## (54) METHOD AND DEVICE FOR MANAGING PERSONAL INFORMATION

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To allow only a specified personal information referencing person designated by a personal information registering person to obtain personal information on-line by outputting personal information corresponding to an enquiry code only when the inputted enquiry code is recognized to be an authentic one.

**SOLUTION:** A method consists of two steps, that is, an enquiry code issuing step where a personal information registering person 71 utilizes a personal information managing device 10 and a personal information obtaining step where a personal information referencing person utilizes the personal information managing device 10. In the enquiry code issuing step, the enquiry code being an identifying code to be inputted by the personal information referencing person, who wants to obtain personal information concerning a certain personal information registering person, is generated by the indication of the personal information registering person so as to be outputted. In the personal information obtaining step, personal information corresponding to the enquiry code is outputted only when it is recognized that the inputted enquiry code is an authentic one which is generated by the issuing step.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 1 4 9 5 0 4

(43) 公開日 平成11年(1999)6月2日

(51) Int. Cl. <sup>6</sup>

G 0 6 F

17/60

15/00

識別記号

3 3 0

F I

G 0 6 F

15/21

15/00

Z

3 3 0 F

審査請求 未請求 請求項の数 1 6

O L

(全 3 1 頁)

(21) 出願番号

特願平9-315473

(22) 出願日

平成9年(1997)11月17日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 高橋 英男

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報・通信開発本部内

(72) 発明者 新田 淳

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報・通信開発本部内

(72) 発明者 田坂 光伸

神奈川県川崎市幸区鹿島田890番地 株式

会社日立製作所情報・通信開発本部内

(74) 代理人 弁理士 小川 勝男

最終頁に続く

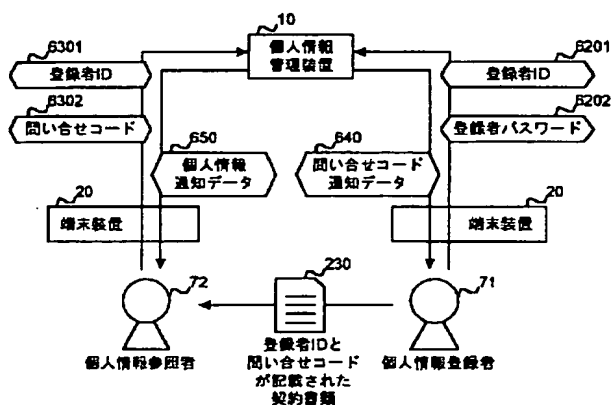
(54) 【発明の名称】 個人情報管理方法および装置

(57) 【要約】

【課題】 住民票データや印鑑証明データなどの個人情報を管理する個人情報管理方法において、個人情報の登録者が指定した個人情報の参照者に対してのみ、個人情報をオンラインで取得することを可能にする。

【解決手段】 個人情報の登録者の指示によって、個人情報を取り出す時に入力する識別データである問い合わせコードを発行する問い合わせコードを発行して個人情報の登録者に通知し、かかる個人情報登録者と対応づけて発行した問い合わせコードを記録しておき、問い合わせコードを通知された個人情報の登録者から発行された問い合わせコードを通知された個人情報の参照者に、個人情報の登録者の識別情報と発行された問い合わせコードを入力させ、入力された問い合わせコードが記録されている問い合わせコードと一致した場合に、かかる登録者に関する個人情報をかかる参照者に出力する。

図 4 3



## 【特許請求の範囲】

【請求項1】個人情報を管理し、上記個人情報の登録者である個人情報登録者の要請によって個人情報の参照者である個人情報参照者にオンラインで上記個人情報登録者に関する個人情報を出力する個人情報管理方法であつて、

個人情報登録者に関する個人情報を取得しようとする個人情報参照者に入力させる識別情報である問い合わせコードを、該個人情報登録者の指示により生成して出力する問い合わせコード発行ステップと、

上記個人情報参照者に上記問い合わせコードを入力させ、入力された問い合わせコードが、上記問い合わせコード発行ステップによって発行された正規の問い合わせコードであると確認された場合に限り、該問い合わせコードに対応する個人情報を出力する個人情報取得ステップとを有することを特徴とする、個人情報管理方法。

【請求項2】請求項1記載の個人情報管理方法において、

前記問い合わせコード発行ステップは、該問い合わせコードの発行を指示する個人情報登録者の本人認証を行う登録者認証ステップと、問い合わせコードを生成する問い合わせコード生成ステップとを有し、

前記個人情報出力ステップは、入力された問い合わせコードが正規の問い合わせコードであることを検定する問い合わせコード検定ステップと、該入力された問い合わせコードに対応する個人情報を出力する個人情報出力ステップとを有することを特徴とする、個人情報管理方法。

【請求項3】請求項2記載の個人情報管理方法において、

前記問い合わせコード生成ステップは、生成した問い合わせコードの記録である問い合わせコード管理情報を記録する問い合わせコード管理情報記録ステップを有し、前記問い合わせコード検定ステップでは入力された問い合わせコードに対応する問い合わせコード管理情報が記録されている場合に、入力された問い合わせコードが有効であると判定することを特徴とする、個人情報管理方法。

【請求項4】請求項3記載の個人情報管理方法において、前記問い合わせコード検定ステップでは、問い合わせコードが有効であると判断した場合に、該問い合わせコード管理情報を抹消することを特徴とする、個人情報管理方法。

【請求項5】請求項3記載の個人情報管理方法において、前記問い合わせコード生成ステップは、前記問い合わせコード管理情報に対応させて、該問い合わせコードの有効期限を記録する有効期限情報を記録する有効期限記録ステップを有し、前記問い合わせコード検定ステップは、前記問い合わせコード管理情報が記録されている場合に、前記有効期限情報に記録されている有効期限を調べる有効期限検査ステップを有し、該有効期限を超過していない場合には該問い合わせコードが有効であると判定し、

該有効期限を超過している場合には該問い合わせコード管理情報と有効期限情報を抹消した上で該問い合わせコードが無効であると判定することを特徴とする、個人情報管理方法。

【請求項6】請求項2記載の個人情報管理方法において、

前記問い合わせコード生成ステップは、前記個人情報登録者が自身に関する個人情報の参照者として指定する個人情報参照者を、前記問い合わせコードと対応づけて記録する参照者指定情報を記録する参照者記録ステップを有し、

前記問い合わせコード検定ステップは、個人情報を取得せんとする個人情報参照者の本人認証を行う参照者認証ステップと、

前記参照者指定情報に記録されている個人情報参照者が、該個人情報を取得せんとする個人情報参照者との一致比較を行う参照者照合ステップを有し、

前記問い合わせコード検定ステップは、前記参照者認証ステップによる本人認証と前記参照者照合ステップによる一致比較が共に成功した場合に限り、入力された問い合わせコードが正しいと判定することを特徴とする、個人情報管理方法。

【請求項7】請求項2記載の個人情報管理方法において、

前記問い合わせコード生成ステップでは、前記個人情報登録者が入力するデータである問い合わせコード平文データに対して、個人情報参照者には公開されていない関数である問い合わせコード生成関数を適用することによって問い合わせコードを生成し、

前記問い合わせコード検定ステップでは、前記個人情報参照者に上記問い合わせコード平文データと前記問い合わせコードの双方を入力させ、前記問い合わせコード生成関数を該問い合わせコード平文データに適用することにより問い合わせコードを再計算し、

該再計算された問い合わせコードと、前記個人情報参照者に入力させた問い合わせコードとを比較し、両者が一致した場合に前記入力された問い合わせコードが有効であると判定することを特徴とする、個人情報管理方法。

【請求項8】請求項7記載の個人情報管理方法において、

前記問い合わせコード生成関数は、複数の異なる関数式が用意されており、前記個人情報登録者に応じて使用する関数式を選択することを特徴とする、個人情報管理方法。

【請求項9】個人情報を管理し、上記個人情報の登録者である個人情報登録者の要請によって個人情報の参照者である個人情報参照者にオンラインで上記個人情報登録者に関する個人情報を出力する個人情報管理装置であつて、

個人情報登録者に関する個人情報を取得しようとする個

個人情報参照者に入力させる識別情報である問い合わせコードを、該個人情報登録者の指示により生成して出力する問い合わせコード発行手段と、

上記個人情報参照者に上記問い合わせコードを入力させ、入力された問い合わせコードが、上記問い合わせコード発行手段によって発行された正規の問い合わせコードであると確認された場合に限り、該問い合わせコードに対応する個人情報を出力する個人情報取得手段とを有することを特徴とする、個人情報管理装置。

【請求項10】請求項9記載の個人情報管理装置において、

前記問い合わせコード発行手段は、該問い合わせコードの発行を指示する個人情報登録者の本人認証を行う登録者認証手段と、問い合わせコードを生成する問い合わせコード生成手段とを有し、

前記個人情報出力手段は、入力された問い合わせコードが正規の問い合わせコードであることを検定する問い合わせコード検定手段と、該入力された問い合わせコードに対応する個人情報を出力する個人情報出力手段とを有することを特徴とする、個人情報管理装置。

【請求項11】請求項10記載の個人情報管理装置において、前記問い合わせコード生成手段は、生成した問い合わせコードの記録である問い合わせコード管理情報を記録する問い合わせコード管理情報記録ステップを有し、前記問い合わせコード検定手段は入力された問い合わせコードに対応する問い合わせコード管理情報が記録されている場合に、入力された問い合わせコードが有効であると判定することを特徴とする、個人情報管理方法。

【請求項12】請求項11記載の個人情報管理装置において、

前記問い合わせコード検定手段は、問い合わせコードが有効であると判断した場合に、該問い合わせコード管理情報を抹消することを特徴とする、個人情報管理装置。

【請求項13】請求項11記載の個人情報管理装置において、

前記問い合わせコード生成手段は、前記問い合わせコード管理情報に対応させて、該問い合わせコードの有効期限を記録する有効期限情報を記録する有効期限記録手段を有し、

前記問い合わせコード検定手段は、前記問い合わせコード管理情報が記録されている場合に、前記有効期限情報に記録されている有効期限を調べる有効期限検査ステップを有し、

該有効期限を超過していない場合には該問い合わせコードが有効であると判定し、

該有効期限が超過している場合には該問い合わせコード管理情報と有効期限情報を抹消した上で該問い合わせコードが無効であると判定することを特徴とする、個人情報管理装置。

【請求項14】請求項10記載の個人情報管理装置にお

いて、

前記問い合わせコード生成手段は、前記個人情報登録者が自身に関する個人情報の参照者として指定する個人情報参照者を、前記問い合わせコードと対応づけて記録する参照者指定情報を記録する参照者記録手段を有し、

前記問い合わせコード検定手段は、個人情報を取得せんとする個人情報参照者の本人認証を行う参照者認証手段と、

前記参照者指定情報に記録されている個人情報参照者

10 が、該個人情報を取得せんとする個人情報参照者との一致比較を行う参照者照合手段を有し、

前記問い合わせコード検定手段は、前記参照者認証手段による本人認証と前記参照者照合手段による一致比較が共に成功した場合に限り、入力された問い合わせコードが正しいと判定することを特徴とする、個人情報管理装置。

【請求項15】請求項10記載の個人情報管理方法において、

前記問い合わせコード生成手段は、前記個人情報登録者が入力するデータである問い合わせコード平文データに対して、個人情報参照者には公開されていない関数である問

20 い合せコード生成関数を適用することによって問い合わせコードを生成し、  
前記問い合わせコード検定手段は、前記個人情報参照者に上記問い合わせコード平文データと前記問い合わせコードの双方を入力させ、前記問い合わせコード生成関数を該問い合わせコード平文データに適用することにより問い合わせコードを再計算し、

該再計算された問い合わせコードと、前記個人情報参照者に入力させた問い合わせコードとを比較し、両者が一致した場合に前記入力された問い合わせコードが有効であると判定することを特徴とする、個人情報管理装置。

30 【請求項16】請求項15記載の個人情報管理装置において、

前記問い合わせコード生成関数は、複数の異なる関数式が用意されており、前記個人情報登録者に応じて使用する関数式を選択することを特徴とする、個人情報管理装置。

【発明の詳細な説明】

【0001】

40 【発明の属する技術分野】本発明は、個人情報を電子的に記憶・管理する装置に係わり、特に、個人情報の登録者が、自身に関する個人情報を参照してよいと許可した特定の第三者に対してのみかかる個人情報をオンラインで提供することが可能な処理方法および装置に関する。さらに好ましくは、住民票や印鑑証明書などの法的な証明能力のある各種の個人情報を、個人情報の登録者が許可した特定の第三者に対してのみオンラインで提供することが可能な処理方法および装置に関する。

【0002】

50 【従来の技術】市役所などの地方自治体では、世帯構成

情報や登録印の印影データなどの個人や法人に関する情報（以後本明細書では総称して個人情報と記す）を電子化して保管しており、かかる個人情報を登録した本人の要請があれば、これらの情報の複写を、住民票や印鑑証明書として交付する業務を行っている。

【0003】現在、これらの証明書類の交付業務を効率化する目的で、磁気ストライプを有するカードによって申請受付事務を自動化することが実現している。この方式では、証明書の自動交付装置に、情報の登録者本人である操作者が磁気カードを挿入し、暗証番号を入力することによって証明書の複写を入手する。自動交付装置は、ホスト計算機上の個人情報データベースに問い合わせ、暗証番号の正当性を確認した上で個人情報を証明書として印刷する。続いて、かかる証明書の改竄を防止するために、証明書としての有効期限と、地方自治体の印を自動的に押印した上で出力する。操作者は、以上の手順で入手した証明書を、典型的には陸運局や公安局などの行政機関や企業に、何らかの届けや契約書類に添付して提出する。それらの行政機関や企業では、証明書に押印された地方自治体の印の正当性を根拠として、かかる証明書の記載内容を信用している。

【0004】上記従来技術に関する発明としては、例えば特開平8-129587の発明がある。

【0005】上記の証明書の自動交付装置による証明書の交付方法には、次のような二つの問題点がある。

【0006】（1）証明書の交付を受けようとする本人が役所に出向いていく必要があり、不便である。

【0007】（2）現行の証明書では、交付後に記載事項に変更が生じうることを考慮して、必ず数ヶ月程度の有効期限が設けられているため、取得した証明書が、利用前に失効した場合には、たとえ記載内容に変更が生じなかったとしても、証明書の再交付を受ける必要があり、不便である。

【0008】上記の2点の問題が生じる原因は、証明書が紙に印刷されているために生じていると言える。もしも、証明書が必要となった時点で証明書に記載する個人情報を保管しているホスト計算機から、かかる個人情報をオンラインで取得して、証明書の代わりに使用することができれば、これらの問題を解決することが可能であると期待できる。

【0009】ところが、かかるホスト計算機をオンライン化し、利用者にホスト計算機へのオンラインアクセスを単純に許可したのでは、以下のような問題が発生してしまい、個人情報をオンラインで取得してそれを証明書の代わりに使用するという目的は達せられない。

【0010】まず、ホスト計算機へのオンラインアクセスを、個人情報を登録した本人（以後本明細書では個人情報登録者と呼ぶ）に許可した場合には、以下の理由により取得された個人情報に、証明書としての証明能力を持たせることができなくなってしまう。すなわち、個人

情報登録者が自身の個人情報をオンラインで取得して、プリンタ等によって印刷したとすると、取得した個人情報を印刷する前に、かかる個人情報登録者がかかる個人情報を改竄する余地が生じてしまうので、印刷された個人情報を証明書として第三者が信用するに足る根拠が生じない。

【0011】一方、ホスト計算機へのオンラインアクセスを、証明書の提出を受ける、行政機関や企業などの第三者（以後本明細書では個人情報参照者と呼ぶ）に許可した場合には、証明書を疑ってかかる立場にある者が、ホスト計算機から直接個人情報を取得するので、個人情報登録者によるデータの改竄が生じる余地はない。ところが今度は、個人情報登録者のプライバシーを保護することができなくなってしまうという別の問題が生じる。すなわち、かかる個人情報参照者は、個人情報登録者の同意なしに、ホスト計算機上の任意の個人情報を自由に参照できてしまうために、個人情報登録者のプライバシーを保護することができない。

【0012】以上の理由により、個人情報を保持したホスト計算機を単純にオンライン化したのでは、得られた個人情報に現行の証明書と同等の証明能力を持たせることができないか、あるいは個人情報登録者のプライバシーを守ることができなくなってしまうために、オンラインで証明書を取得するという目的は達せられない。

【0013】既存技術を用いて従来技術がかかえる問題点の解決を試みる別の案として、例えば「PGP:Pretty Good Privacy」（Simson Garfinkel, O'Reilly & Associates Inc.）のpp. 218-227に紹介されているようなデジタル署名技術を単純に適用して個人情報の改竄を防止しようとすることも考えられるが、この場合には以下の理由により、紙に書かれた現行の各種契約書類との相性が悪いために、個人情報登録者または個人情報参照者に不便を強いることになる。

【0014】もしも市役所等が紙に印刷した証明書に代わって、デジタル署名を付した個人情報を格納した記憶媒体を個人情報登録者に交付したとすると、個人情報登録者は、従来紙に印刷された証明書を個人情報参照者に提出していたかわりに、かかる記憶媒体を提出する必要が生じる。現在一般的には、個人情報登録者は、個人情報参照者に、紙に書かれた何らかの契約書類に添えて証明書を提出するので、数種類の書類をまとめて提出するだけでよい現行の形式にくらべて、紙の契約書類に混じって電子的な記憶媒体を提出しなければならないのは個人情報登録者にとって煩わしい。ここでさらに、電子的な記憶媒体の介在をなくすことを意図して、デジタル署名の付されたデータを、前掲書のp. 224に示されるような形式で、紙に印刷するようにしたとしても、個人情報参照者がかかる印刷された個人情報の正当性を検証するためには、印刷内容を元の電子化されたデータに変換して、電子署名の検証機能を有する装置に入力しなけ

ればならないので、結局個人情報参照者に多大な手間を要求してしまう。各種の契約書類が電子化され、契約書類の提出自体がオンライン化されれば、証明書類データをデジタル署名の付されたデータとしてオンラインで授受することも現実味を帯びるが、当分の間は紙に記載された契約書類が使用され続けることが予想される。以上の理由により、デジタル署名により個人情報の改竄を防止する方法は、紙に書かれた現行の各種契約書類との相性が悪く、契約書類自身が電子化されるまでの間は、個人情報登録者や個人情報参照者に不便を強いることになる。

#### 【0015】

【発明が解決しようとする課題】本発明は、上記の事情に鑑みてなされたもので、以下の課題を解決することを目的とする。すなわち、住民票データや印鑑証明データを始めとする個人情報を管理し、個人情報の持ち主の要請によって個人情報データを出力する個人情報管理装置において、

(1) 個人情報登録者が指定する特定の個人情報参照者に対してのみ、個人情報をオンラインで取得させることを可能にする。

【0016】(2) 個人情報登録者と、上記の特定の個人情報参照者との間で、電子化されたデータを授受する必要をなくす。

#### 【0017】

【課題を解決するための手段】本発明は上記の課題を解決するために、世帯構成情報や登録印の印影データを始めとする個人情報を管理し、個人情報の持ち主の要請によって個人情報を出力するオンライン化された個人情報管理装置の個人情報管理方法において、ある個人情報登録者に関する個人情報を取得しようとする個人情報参照者に入力させる識別情報である問い合わせコードを、該個人情報登録者の指示により生成して出力する問い合わせコード発行ステップと、上記個人情報参照者に上記問い合わせコードを入力させ、入力された問い合わせコードが、上記問い合わせコード発行ステップによって生成された正規の問い合わせコードであると確認された場合に限り、該問い合わせコードに対応する個人情報を出力する個人情報取得ステップを有するようにしている。

【0018】また、前記問い合わせコード発行ステップは、問い合わせコード発行ステップを実行させている操作者が個人情報登録者本人であることを認証する個人情報登録者認証ステップと、問い合わせコードを生成する問い合わせコード生成ステップを有するようにしている。

【0019】また、前記個人情報取得ステップは、入力された問い合わせコードが、正規の問い合わせコード発行ステップによって発行された問い合わせコードであるかどうかを検定する問い合わせコード検定ステップと、該問い合わせコードに対応する個人情報を出力する個人

情報出力ステップとを有するようにしている。

【0020】本発明では、上記問い合わせコード発行ステップにおいて、問い合わせコードは個人情報登録者本人が操作した場合にのみ発行されるので、個人情報登録者本人以外の者が無断で問い合わせコード発行処理を実行させることは不可能である。すなわち、問い合わせコードは、個人情報登録者本人の要請によってのみ発行される。

【0021】一方、上記個人情報出力ステップでは、特定の個人情報登録者に関する個人情報を取得しようとする個人情報参照者は、対応する問い合わせコードを入力しなければならないが、かかる問い合わせコードを入手するには上記問い合わせコード発行ステップを実行させる他ない。すなわち、個人情報登録者本人が問い合わせコード発行ステップを実行させて、発行された問い合わせコードを通知してもらった場合にのみ、個人情報参照者はかかる個人情報を取得することが可能となる。これにより、個人情報登録者が指定する特定の個人情報参照者に対してのみ、個人情報をオンラインで取得させることを可能にするという本発明の第一の目的は達せられる。

【0022】また、問い合わせコードには、処理の通し番号や乱数によって生成した暗証番号など、書類等に人手で記入するのに不自由のない長さのデータを用いることが可能であるため、個人情報登録者が問い合わせコードを通知するのに、電子化されたデータを受け渡す必要がない。これにより、個人情報登録者と、上記の特定の個人情報参照者との間で、電子化されたデータを授受する必要をなくすという、本発明の第二の目的は達せられる。

#### 【0023】

【発明の実施の形態】《第一の実施例》以下に、本発明の一実施例を図面を用いて詳細に説明する。

【0024】まず、本発明の動作説明図である図43を用いて、本実施例の構成と動作の概要について説明する。本実施例では、個人情報登録者71と個人情報参照者72の両者は端末装置20を介して個人情報管理装置10を利用する。

【0025】本発明の典型的な適用例では、個人情報参照者72は個人情報登録者71が提出する何らかの契約書類230の記載事項を、市役所などが発行する住民票などの証明書類とつきあわせて確認したいと考える立場にある事業者である。以下ではかかる個人情報登録者71が本発明を利用して、個人情報参照者72に契約書類230の正当性を確認させるに至る手順を説明する。

【0026】本装置の利用手順は、個人情報登録者71が個人情報管理装置10を利用するフェーズである問い合わせコード発行フェーズと、個人情報参照者が個人情報管理装置10を利用する個人情報取得フェーズとの二つのフェーズからなる。

【0027】まず、問い合わせコード取得フェーズにおいて個人情報登録者71は、端末装置20を介して個人情報管理装置10に、自身の識別子である登録者ID6201と、自身を認証する登録者パスワード6202を入力し、自身に関する個人情報を第三者に提示する意志があることを個人情報管理装置10に通知する。個人情報管理装置10は登録者ID6201と登録者パスワード6202を照合することにより、個人情報登録者71本人が確かに要求を送信していることを確認した上で、後の個人情報取得フェーズでかかる個人情報登録者71に関する個人情報を取得することを許可するパスワードとして機能する問い合わせコードを発行し、問い合わせコード通知データ640として端末装置20に返送する。端末装置20より出力された問い合わせコード通知データ640を入手した個人情報71は、自身の登録者IDと、発行された問い合わせコードを契約書類230に記入した上で、かかる契約書類230を個人情報参照者72に渡す。

【0028】次に、個人情報取得フェーズにおいて個人情報参照者は、契約書類230の記載内容に従って、登録者ID6301と問い合わせコード6302を端末装置20に入力して個人情報管理装置10に送信して、登録者ID6301に対応する個人情報を参照する意志があることを伝える。個人情報管理装置10はかかる登録者ID6301に対応する個人情報登録者が、個人情報の提示に同意しているかどうかを確認するために、登録者ID6301と問い合わせコード6302の対応を調べる。調べた結果、入力された問い合わせコード6302が、問い合わせコード発行フェーズにおいて発行された問い合わせコードであることを確認できた場合に限り、登録者ID6301に対応する個人情報を個人情報通知データ650として端末装置20に送信する。個人情報参照者72は、端末装置20から出力された個人情報通知データ650と、契約書類230の記載内容を照合することにより、契約書類230の記載内容を確認することができる。

【0029】以上の手順によれば、問い合わせコード発行フェーズにおいて特定の個人情報登録者71に対応する問い合わせコードを発行させることができるのは登録者パスワード6202を知っている個人情報登録者71本人に限られるので、第三者が勝手に問い合わせコードを発行させることは不可能である。また、個人情報取得フェーズにおいては、個人情報参照者は、参照しようとする個人情報登録者71に対応した登録者ID6301を入力しなければならないので、個人情報登録者71から問い合わせコードを入手しなければかかる個人情報を参照することは不可能である。結局、個人情報登録者71が自身に関する個人情報を参照させようと考えた個人情報参照者72だけが、かかる個人情報を参照することが可能となる。

【0030】一方、個人情報参照者72は個人情報管理

装置10から直接個人情報通知データ650をオンラインで取得するので、得られた個人情報通知データ650の内容は、現行の各種証明書類と同程度に信用することができる。

【0031】次に、本実施例の構成とその動作について詳細に説明する。

【0032】本実施例では、個人情報管理装置をパーソナルコンピュータ（以下パソコン）などの汎用の計算機と、その上で実行されるHTTP（Hyper Text Transfer Protocol）サーバプログラムによって構成している。また、個人情報登録者や個人情報参照者（両者を併せて以下では利用者と呼ぶ）が利用する端末装置として、パソコンなどの汎用の計算機と、その上で実行される汎用のHTTPクライアントプログラム（以下ではブラウザと呼ぶ）で構成している。個人情報管理装置と端末装置の間の通信プロトコルとしては、本実施例では既存の汎用の通信プロトコルであるHTTPを使用する。以下の説明では、通信プロトコルとしてHTTPを用いた構成について説明するが、上記の通信プロトコルとしては、メニュー画面を端末装置上に表示させ、ユーザに処理を選択させたりデータを入力させることが可能なプロトコルであれば他の汎用の通信プロトコルや独自の専用プロトコルを用いることも可能である。例えば、テキストデータをそのまま送受信するパソコン通信形式のプロトコルを用いてもかまわない。本実施例では、個人情報管理装置10上ではHTTPサーバプログラムを実行し、端末装置20上では汎用のHTTPクライアントプログラム（以下ではブラウザと呼ぶ）を実行させるものとして説明する。

【0033】また、本実施例では、個人情報管理装置が管理する個人情報の一例として住民票データを取り上げるが、同様にして例えば印鑑証明データなどの他の形式の個人情報を管理することが可能である。

【0034】また、本実施例では、問い合わせコードを乱数により生成するが、問い合わせコードとしては、乱数以外であっても、プログラムやハードウェアによる生成が可能であり、第三者による推定が困難なデータが得られれば他の方法によって生成してもよい。

【0035】また、本実施例では問い合わせコードを個人情報登録者ごとに発行する。すなわち、特定の個人情報登録者に対して発行される複数の問い合わせコードはそれぞれ別の値を取るが、異なる個人情報登録者に対して発行される別々の問い合わせコードが同一の値を取る場合がありえる。そのため、問い合わせコードに対応させてなんらかの情報を記録するテーブルを設ける場合には、個人情報登録者の識別子である登録者IDと問い合わせコードの組をテーブルのキーとして用いるようにしている。

【0036】図1は、本発明が提供する個人情報管理装置のシステム構成図である。図1において、本発明が提供する個人情報管理装置10は、ネットワーク30を経

由して端末装置20に接続されている。個人情報管理装置10は端末装置20を操作する利用者が入力する入力データ210に応じて、問い合わせコードを発行する処理と、個人情報を出力する処理のいずれかを実行して、出力データ220として利用者に提供する。

【0037】個人情報管理装置10と端末装置20はそれぞれ、パーソナルコンピュータ（以下パソコン）などの汎用の計算機と、その上で実行するプログラムにより構成している。

【0038】図2は、個人情報管理装置10の構成図である。図2において、個人情報管理装置10は、CPU110と、ネットワークインタフェース回路120と、二次記憶装置制御回路130と主記憶装置140と二次記憶装置150から構成される。ネットワークインタフェース回路120はCPU110の指示に従い、端末装置20上のブラウザとやりとりするネットワーク30上のメッセージを送受信する。二次記憶装置130は、二次記憶装置150に接続されており、CPU110からの指示に従い、二次記憶装置150上にデータを入出力する。主記憶装置140上には、端末装置20を操作する個人情報登録者の指示に応じて問い合わせコードを発行する問い合わせコード発行プログラム1420と、問い合わせコード発行プログラム1420が使用するワークエリア1440と、端末装置20を操作する個人情報参照者の指示に応じて個人情報を出力する個人情報出力プログラム1430と、個人情報出力プログラム1430が使用するワークエリア1450と、端末装置20から送られてくるメッセージに応じて、各種の画面データを端末装置20に送信する処理と、問い合わせコード発行プログラム1420や個人情報出力プログラム1430を起動し、それらの出力結果を端末装置20に返送する処理を実行する通信制御プログラム1410と、問い合わせコード発行プログラム1420や個人情報出力プログラム1430の指示に応じて二次記憶装置150上の各種のテーブルを管理するテーブル管理プログラム1460と、個人情報管理装置10のハードウェア資源を管理するOS1470が格納される。OS1470は装置の起動時に自動的に起動され、通信制御プログラム1410を起動する。一旦起動されると通信制御プログラム1410は、端末装置からのメッセージを受信するために待機する。

【0039】上記の構成において、OS1470としては、市販の汎用OSを使用することが可能であり、テーブル管理ライブラリ1460としては、市販のデータベース管理ライブラリを利用することが可能であり、通信制御プログラム1410としては、市販の汎用のHTTPサーバプログラムを使用することが可能である。一方、問い合わせコード発行プログラム1420と個人情報出力プログラム1430は、本実施例で詳細に説明する処理内容をプログラムとして実装することによって実

現することが可能である。

【0040】問い合わせコード発行プログラム1420と、個人情報出力プログラム1430は、二次記憶装置150上に格納した各種のテーブルを参照ないし更新する際に、テーブル管理ライブラリ1460を呼び出す。以下の説明ではこれら個々の呼び出しは自明であるため特に明記しない。同様に、各プログラムおよびライブラリからの、OS1470が提供するシステムコールの呼び出しについても特に明記しない。

10 【0041】問い合わせコード発行プログラム1420は、個人情報登録者が端末装置20上の画面の案内に従って問い合わせコード発行処理を指示した場合に、通信制御プログラム1410によって起動され、個人情報登録者が端末装置20に入力した入力データ210に基づいて問い合わせコードを生成し、生成した問い合わせコードを、端末装置20が出力可能な形式の問い合わせコード通知データに変換して出力する。通信制御プログラム1410は、出力された問い合わせコード通知データを端末装置20に送り返し、端末装置20はこれを個人情報登録者に表示する。

20 【0042】個人情報出力プログラム1430は、個人情報参照者が端末装置20の画面の案内に従って個人情報の出力処理を指示した場合に、通信制御プログラム1410によって起動され、個人情報参照者が端末装置20に入力したデータに対応する個人情報を検索し、検索した個人情報を、端末装置20が出力可能な形式の個人情報通知データに変換して出力する。通信制御プログラム1410は、出力された個人情報通知データを端末装置20に送り返し、端末装置20はこれを個人情報参照者に表示する。

30 【0043】次に、図3を用いて二次記憶装置150に格納する情報について説明する。本実施例では、二次記憶装置150に、住民票データを格納したテーブルである個人情報テーブル1510と、発行した問い合わせコードを管理する問い合わせコード管理テーブル1520と、個人情報登録者の登録者IDと登録者パスワードを管理する登録者管理テーブル1530と、通信制御プログラム1410が端末装置20に送り返す定型の画面データを格納した複数のファイルからなる画面データファイル群1590を格納している。なお、本実施例では、個人情報管理装置10が管理する個人情報の一例として住民票データを取り上げ、個人情報テーブル1510には住民票データを格納するが、同様の構成によって印鑑証明データなどの他の形式の個人情報を格納することも可能である。

【0044】次に上記の各テーブルの構成について説明する。

【0045】図4は、個人情報管理テーブル1510の構成図である。個人情報管理テーブル1510は、個人情報管理装置10が管理する個人情報を記憶・管理する



テーブルであり、本実施例では個人情報の一例として住民票データを格納している。本テーブルは、個人情報登録者の識別子である登録者IDを格納する登録者IDフィールド1511と、住民票データを構成する住所フィールド1512や、世帯主氏名フィールド1513等のフィールドを有する。本テーブルは登録者IDフィールド1511をキーとして検索することにより、該当する個人情報登録者の住民票データを得ることができる。本テーブルへのデータの登録や更新のためのプログラムや操作手順は、本発明と関係ないので説明を省略する。

【0046】図5は、問い合わせコード管理テーブル1520の構成図である。問い合わせコード管理テーブル1520は、発行済みの問い合わせコードを管理するテーブルであり、問い合わせコード発行処理を指示した個人情報登録者の登録者IDを記録する登録者IDフィールド1521と、発行した問い合わせコードを記録する問い合わせコードフィールド1522とを有する。本テーブルは登録者IDフィールドと問い合わせコードフィールド1522の組をキーとしており、登録者IDと問い合わせコードの組がレコードとして存在すれば、かかる登録者IDと問い合わせコードの組み合わせは有効であると見なせる。本テーブルのレコードは問い合わせコード発行処理において作製され、個人情報取得処理において参照された後に削除される。

【0047】図6は、登録者管理テーブル1530の構成図である。登録者管理テーブル1530は、個人情報登録者を認証するために登録者IDと登録者パスワードを対応づけて管理するためのテーブルであり、個人情報登録者の一意な識別子である登録者IDを格納する登録者IDフィールド1531と、該登録者IDに対応するパスワードである登録者パスワードを格納する登録者パスワードフィールド1532を有する。本テーブルは、登録者IDフィールド1531をキーとして検索することによって対応する登録者パスワードフィールド1532を知ることができる。本テーブルを管理するためのプログラムや操作手順は、本発明と関係ないので説明を省略する。

【0048】図7は、画面データファイル群1590の構成図である。画面データファイル群1590は、通信制御プログラム1410が端末装置20に送り返す定型の画面データを格納したファイルの集まりであり、処理選択画面データファイル1591と、問い合わせコード発行申請画面データファイル1592と、個人情報出力申請画面データファイル1593から構成される。処理選択画面データファイル1591は、端末装置20の利用者に問い合わせコード発行処理と個人情報出力処理から実行する処理を選択させる画面である処理選択画面に対応するファイルである。問い合わせコード発行申請画面データファイル1592は、上記の利用者が問い合わせコード発行処理を選択した場合に表示される画面であ

る問い合わせコード発行申請画面に対応するファイルである。個人情報出力申請画面データファイル1593は、上記の利用者が個人情報出力処理を選択した場合に表示される画面である個人情報出力申請画面に対応するファイルである。

【0049】本実施例ではこれらの画面データファイルはHTML(Hypertext Markup Language)言語で記述されたHTMLページファイルであり、HTML言語が提供するリンク機能により、画面上のボタンを利用者が選択することによって画面が切り替わるように記述されている。これらの各データファイルが、端末装置20の画面に表示される時の表示形式を次に説明する。

【0050】図8は、処理選択画面データファイル1591が、端末装置20で表示されたときの画面である処理選択画面610の構成図である。本画面は、利用者が端末装置20を通して個人情報管理装置10を利用する時に端末装置20に最初に表示される画面であり、処理の選択を促す説明文と、問い合わせコード発行処理の実行を指示する問い合わせコード発行ボタン6111と、個人情報出力処理の実行を指示する個人情報出力ボタン6112を有する。それぞれのボタンは、別の画面データを取得することをブラウザに指示する指令であるHTMLリンクとして構成されており、問い合わせコード発行申請ボタン6111は、問い合わせコード発行申請画面データファイル1592へのリンクとして、また、個人情報取得ボタン6112は個人情報取得申請画面データファイル1593へのリンクとして構成されている。利用者がいずれかのボタンを選択した場合には、端末装置20上のブラウザは、個人情報管理装置10上の通信制御プログラム1410に、ボタンに関連付けられたリンクに対応するデータファイルを送信させ、かかるデータファイルを端末装置20の画面上に表示する。

【0051】図9は、問い合わせコード発行申請画面データファイル1592が、端末装置20に表示された時の画面である問い合わせコード発行申請画面620の構成図である。本画面は、端末装置20の利用者である個人情報登録者が、処理選択画面610において問い合わせコード発行ボタン6111を選択した場合に表示され、画面上には、登録者IDを入力させる登録者ID入力欄6201と、対応する登録者パスワードを入力させる登録者パスワード入力欄6202と、これらの入力欄に入力されたデータの送信を指示する発行ボタン6209を有する。これらの入力欄とボタンは入力データを通信制御プログラム1410に送信して所定のプログラムを実行させる指令であるHTMLのデータ入力フォームとして構成されており、発行ボタン6209を利用者が選択した場合には各入力欄の入力内容を送信した上で問い合わせコード発行プログラム1420が起動されるように、問い合わせコード発行申請画面データファイル1

592は記述されている。

【0052】図10は、個人情報出力申請画面データファイル1593が、端末装置20に表示された時の画面である個人情報出力申請画面630の構成図である。本画面は、端末装置20の利用者である個人情報参照者が、処理選択画面610において個人情報出力ボタン6112を選択した場合に表示され、画面上には、出力させたい個人情報に対応する個人情報登録者の登録者IDを入力するための登録者ID入力欄6301と、かかる個人情報登録者から個人情報参照者が通知されたが上記の問い合わせコード発行処理の結果入手した問い合わせコードを入力するための問い合わせコード入力欄6302と、これらの入力欄に入力されたデータの送信を指示する取得ボタン6309を有する。これらの入力欄とボタンはHTMLのデータ入力フォームとして構成されており、取得ボタン6309を利用者が選択した場合にはそれぞれの入力欄の入力データを送信した上で個人情報出力プログラム1430が起動されるように、個人情報出力申請画面データファイルは記述されている。

【0053】図11は、問い合わせコード発行プログラム1420の出力である問い合わせコード通知データが、端末装置20で表示された時の画面である問い合わせコード通知画面640の構成図である。本画面は、問い合わせコード発行申請画面620において個人情報登録者が自身の登録者ID6201と登録者パスワード6202を入力し、発行ボタン6209を選択した場合に表示される。本画面には、発行された問い合わせコードが表示される。

【0054】図12は、個人情報出力プログラム1430の出力である個人情報通知データが、端末装置20で表示された時の画面である個人情報通知画面650の構成図である。本画面は、個人情報出力申請画面630において個人情報参照者が登録者ID6301と問い合わせコード6302を入力し、取得ボタン6309を選択した場合に表示される。本画面には出力された個人情報が表示される。

【0055】次に、問い合わせコード発行プログラム1420の処理内容について説明する。問い合わせコード発行プログラム1420は、端末装置20の利用者が、問い合わせコード発行申請画面620において発行ボタン6209を選択した場合に、通信制御プログラム1410により起動される。問い合わせコード発行プログラム1420の入力は問い合わせコード発行申請画面620のそれぞれの入力欄に利用者である個人情報登録者が入力したデータであり、出力は、処理に成功した場合には、問い合わせコード通知画面640に対応する問い合わせコード通知データであり、失敗した場合には図示しないエラー画面に対応するエラー通知データである。本プログラムは、登録者パスワード6202が正しい場合にのみ処理に成功する。本プログラムの出力は通信制御

プログラム1410により端末装置20に返送され、端末装置20上のブラウザにより画面上に表示される。問い合わせコード発行プログラムの具体的な処理内容を図13に示すPAD図に沿って説明する。

【0056】(ステップ50101) 問い合わせコード発行プログラム1420は、入力された登録者ID6201、登録者パスワード6202をワークエリア1440に格納する。

【0057】(ステップ50102) 問い合わせコード発行プログラム1420は、登録者ID6201と登録者パスワード6202を照合する個人情報登録者認証ルーチン14210を呼び出して、戻り値としてパスワードの正否を示す論理値を得る。

【0058】(ステップ50103) 問い合わせコード発行プログラム1420は、個人情報登録者認証ルーチン14210の戻り値がTRUE、すなわちパスワードが正しかった場合にはステップ50104～50105を実行し、戻り値がFALSE、すなわちパスワードが正しくなかった場合にはステップ50106を実行する。

【0059】(ステップ50104) 問い合わせコード発行プログラム1420は、登録者ID6202に対応した問い合わせコードを発行する問い合わせコード生成ルーチン14220を呼び出して、問い合わせコードを生成させ、戻り値として生成された問い合わせコードを得る。

【0060】(ステップ50105) 問い合わせコード発行プログラム1420は、問い合わせコード生成ルーチン14220の戻り値の問い合わせコードを元に、問い合わせコード通知画面640に対応する問い合わせコード通知データを生成して通信制御プログラム1410に出力する。

【0061】(ステップ50106) 問い合わせコード発行プログラム1420は、パスワードが正しくないために処理が拒絶された旨を告げる、図示しないエラー通知データを通信制御プログラム1410に出力する。

【0062】本プログラムは端末装置20に表示された問い合わせコード発行申請画面620に、利用者が登録者ID6201と登録者パスワード6202を入力して発行ボタン6209を選択した場合に起動され、登録者ID6201と登録者パスワード6202が正しい場合にのみ問い合わせコードを生成して問い合わせコード通知データを出力する。すなわち、端末装置20を操作して本プログラムを起動し、問い合わせコードを生成させることができるのは、正しい登録者パスワードを知っている個人情報登録者本人に限られ、登録者パスワードが知られてしまわない限りは、第三者が個人情報登録者に成り代わって問い合わせコードを発行させることはできない。

【0063】次に、問い合わせコード発行プログラムが呼

び出すサブルーチンである個人情報登録者認証ルーチン 14210 と問い合わせコード生成ルーチン 14220 の処理内容について具体的に説明する。

【0064】まず、一つ目のサブルーチンである個人情報登録者認証ルーチン 14210 について説明する。個人情報登録者認証ルーチン 14210 は、ワークエリア 1440 に格納された登録者 ID6201 と登録者パスワード 6202 を入力とし、入力された登録者パスワード 6202 を、登録者管理テーブル 1530 に記録されている登録者パスワードフィールド 1532 の内容と照合することによって個人情報登録者を認証するルーチンである。個人情報登録者認証ルーチン 14210 の処理の各ステップを図 14 に示す PAD 図に従って説明する。

【0065】(ステップ 50201) 個人情報登録者認証ルーチン 14210 は、登録者 ID6201 をキーとして登録者管理テーブル 1530 のレコードを検索する。

【0066】(ステップ 50202) 個人情報登録者認証ルーチン 14210 は、該レコードが存在して、かつ該レコードのパスワードフィールド 1532 の内容と、利用者が入力したパスワード 6202 が一致する場合には入力された登録者パスワードが正しいことを意味する TRUE を返し、両者が一致しないか、そもそも上記レコードが存在しない場合には正しくないことを示す FALSE を返す。

【0067】次に、二つ目のサブルーチンである問い合わせコード生成ルーチン 14220 について説明する。問い合わせコード生成ルーチン 14220 は、問い合わせコードを生成して、生成した問い合わせコードを問い合わせコード管理テーブル 1530 に記録した上で戻り値として返すルーチンである。本ルーチンは登録者 ID6201 と登録者パスワード 6202 の対応が認証された後に問い合わせコード発行プログラム 1420 より起動される。本実施例では、問い合わせコードの生成方法の例として乱数を利用する方法を示すが、乱数以外であっても、プログラムや装置による生成が可能であり、第三者による推定が困難なデータを生成できればどのような生成方法を用いてもかまわない。問い合わせコード生成ルーチン 14220 の処理の各ステップを図 15 に示す PAD 図に従って説明する。

【0068】(ステップ 50301) 問い合わせコード生成ルーチン 14220 は、6 桁の乱数値を生成して問い合わせコードとする。

【0069】(ステップ 50302) 問い合わせコード生成ルーチン 14220 は、生成した問い合わせコードと、登録者 ID6201 の組からなるレコードを問い合わせコード管理テーブル 1520 から検索する。

【0070】(ステップ 50303) 問い合わせコード生成ルーチン 14220 は、上記レコードが存在した場

合、すなわち、登録者 ID6201 に対応してすでに同一の問い合わせコードが発行済みである場合には、問い合わせコードの重複を避けるためにステップ 50301 から処理をやりなおす。

【0071】(ステップ 50304) 問い合わせコード生成ルーチン 14220 は、生成した問い合わせコードと、登録者 ID6201 の組をレコードとして問い合わせコード管理テーブル 1520 に追加する。

【0072】(ステップ 50305) 問い合わせコード生成ルーチン 14220 は、生成した問い合わせコードを戻り値として返して終了する。

【0073】以上説明した二つのサブルーチンを利用して問い合わせコード発行プログラム 1420 は問い合わせコード発行処理を実行する。

【0074】次に、個人情報出力プログラム 1430 の処理内容について説明する。個人情報出力プログラム 1430 は、端末装置 20 の利用者が、個人情報出力申請画面 630 において取得ボタン 630 を選択した場合に、通信制御プログラム 1410 により起動される。個人情報出力プログラム 1430 の入力 is 個人情報出力申請画面 630 のそれぞれの入力欄に入力されたデータであり、出力は、問い合わせコード 6302 が正しかった場合には個人情報通知画面 650 に対応する個人情報通知データであり、問い合わせコード 6302 が正しくなかった場合には図示しないエラー通知データである。本プログラムの出力は通信制御プログラム 1410 により端末装置 20 に返送され、端末装置 20 上のブラウザにより画面に表示される。個人情報出力プログラム 1430 の処理内容を図 16 に示す PAD 図に従って説明する。

【0075】(ステップ 50401) 個人情報出力プログラム 1430 は、入力された登録者 ID6301 と問い合わせコード 6302 をワークエリア 1450 に格納する。

【0076】(ステップ 50402) 個人情報出力プログラム 1430 は、入力された問い合わせコード 6302 を検定する問い合わせコード検定ルーチン 14310 を呼び出して、登録者 ID6301 と問い合わせコード 6302 を照合し、戻り値として検定の成否を表す論理値を得る。

【0077】(ステップ 50403) 個人情報出力プログラム 1430 は、問い合わせコード検定ルーチン 14310 の戻り値が FALSE、すなわち入力された問い合わせコードが不正である場合には、図示しないエラー画面を端末装置に出力させるエラー通知データを通信制御プログラム 1410 に出力して終了する (ステップ 50404)。

【0078】(ステップ 50405) 個人情報出力プログラム 1430 は、個人情報テーブル 1510 から登録者 ID6301 に対応するレコードを読み出し、ワークエリア 1450 に格納する。

【0079】(ステップ50406) 個人情報出力プログラム1430は、読み出したレコードの内容である個人情報、個人情報通知画面650に対応する個人情報通知データに変換して通信制御プログラム1410に出力する。

【0080】以上説明した処理内容により、個人情報出力プログラム1430は、端末装置20に表示された個人情報出力申請画面630に、利用者が登録者ID6301と問い合わせコード6302を入力して取得ボタン6309を選択した場合に起動され、登録者ID6301と問い合わせコード6302が正しく対応する場合にのみ、登録者ID6301に対応する個人情報を個人情報通知データとして出力する。すなわち、端末装置20を操作して本プログラムを起動し、個人情報通知データを出力させることができるのは、正しい問い合わせコードを知っている個人情報登録者本人か、個人情報登録者から問い合わせコードを通知された個人情報参照者に限られ、問い合わせコードが知られてしまわない限りは、第三者が個人情報登録者に無断で個人情報を出力させることはできない。

【0081】次に、個人情報出力プログラム1430が呼び出すサブルーチンである問い合わせコード検定ルーチン14310とと使用済みレコード削除ルーチン14320の処理内容について具体的に説明する。

【0082】まず、一つ目のサブルーチンである問い合わせコード検定ルーチン14310について説明する。問い合わせコード検定ルーチン14310は、ワークエリア1450に格納された登録者ID6301と問い合わせコード6302を、問い合わせコード管理テーブル1520と照合して、問い合わせコード6302が正しい場合にはTRUE、正しくない場合にはFALSEを返す。さらに、問い合わせコードが正しい場合には、該問い合わせコードを以後無効とするために該問い合わせコードに対応するレコードを問い合わせコード管理テーブル1520から削除する。問い合わせコード検定ルーチン14310の具体的な処理内容を図17に示すPAD図に従って説明する。

【0083】(ステップ50501) 問い合わせコード検定ルーチン14310は、入力された問い合わせコード6302と登録者ID6301の対からなるレコードを問い合わせコード管理テーブル1520から検索する。

【0084】(ステップ50502) 問い合わせコード検定ルーチン14310は、上記レコードが存在しない、すなわち問い合わせコード6302が正しくなければ問い合わせコードが正しくないことを意味するFALSEを戻り値として返して終了する(ステップ50503)。

【0085】(ステップ50504) 問い合わせコード検定ルーチン14310は、上記レコードを削除して、問い合わせコード6302を無効にする。

【0086】(ステップ50505) 問い合わせコード検

定ルーチン14310は、問い合わせコードが正しいことを意味するTRUEを戻り値として返して終了する。

【0087】次に、以上説明したように構成された個人情報管理装置10の動作について、個人情報登録者と個人情報参照者のそれぞれが、本発明を利用して個人情報を出力させる場合の利用者の操作手順に沿って説明する。

【0088】まず、個人情報登録者が問い合わせコードの発行を受けるための操作手順について説明する。個人情報登録者は、端末装置20を操作するに先立ち、個人情報管理装置の運営主体に住民票情報を登録しておき、登録者IDと登録者パスワードの発行を受けておく。運用主体は、個人情報を個人情報管理テーブル1510に、登録者IDと登録者パスワードを登録者管理テーブル1530に登録しておくが、これらの登録処理は本発明とは直接関係ないので詳細な説明は省略する。

【0089】以上の事前準備を済ませた上で個人情報登録者は端末装置20上のブラウザを起動し、個人情報管理装置10のネットワーク上でのアドレスを入力する。

するとブラウザには処理選択画面610が表示される。個人情報登録者はここで問い合わせコード発行ボタン6111を押す。すると、問い合わせコード発行申請画面620が表示される。この画面において個人情報登録者は、事前に発行された自身の登録者IDと登録者パスワードをそれぞれ登録者ID入力欄6201と登録者パスワード入力欄6202にそれぞれ入力し、発行ボタン6209を選択する。この操作により、それぞれの入力欄の入力データはブラウザによって通信制御プログラム1410に送信され、通信制御プログラム1410は受信した入力データを渡して問い合わせコード発行プログラム1420を起動する。起動された問い合わせコード発行プログラム1420は、入力された登録者IDと登録者パスワードが正しければ問い合わせコードを生成し、生成した問い合わせコードを、ブラウザが表示可能な問い合わせコード通知データとして出力する。問い合わせコード通知データは通信制御プログラム1410が端末装置20に返送し、端末装置20は、問い合わせコード通知画面640として表示する。個人情報登録者は問い合わせコード通知画面640に表示された問い合わせコードを手で書きとめるか、画面をプリンタによって印刷するなどして記録する。上記の一連の手順においてももしも登録者パスワードが正しくなかった場合には問い合わせコード通知データの代わりにエラー通知データが出力され、端末装置20には図示しないエラー通知画面が表示される。

【0090】以上の処理が正常に終了した場合には、かかる個人情報登録者は、自身の登録者IDと発行された問い合わせコードを個人情報参照者に通知する。個人情報参照者は、通知された登録者IDと問い合わせコードを用いて、以下に説明する手順で上記個人情報登録者に関する個人情報を取得する。

【0091】個人情報参照者は、端末装置20上のブラウザを起動し、個人情報管理装置10のネットワーク上でのアドレスを入力する。するとブラウザには処理選択画面610が表示される。個人情報参照者はここで個人情報取得ボタン6112を選択する。すると、個人情報出力申請画面630が表示される。この画面において個人情報参照者は、上記個人情報登録者より通知された登録者IDと問い合わせコードをそれぞれ登録者ID入力欄6301と問い合わせコード入力欄6302に入力し、取得ボタン6309を選択する。この操作により、それぞれの入力欄の入力データはブラウザによって通信制御プログラム1410に送信され、通信制御プログラム1410は、受信した入力データを渡して個人情報取得プログラム1430を起動する。個人情報取得プログラム1430は、入力された登録者ID6301と問い合わせコード6302の組み合わせが正しければ、上記個人情報登録者に関する個人情報を検索し、それを端末装置20によって出力することが可能な個人情報通知データとして出力する。個人情報通知データは通信制御プログラムが端末装置20に送信し、端末装置20はそれを個人情報通知画面650として表示する。

【0092】上記の一連の手順においてももしも個人情報参照者が入力した問い合わせコード6302が正しくなかった場合には、端末装置20の画面上には個人情報通知画面650の代わりに図示しないエラー画面が表示される。以上の手順により、個人情報参照者は個人情報登録者に関する個人情報を取得することができる。

【0093】また、本実施例では、個人情報出力プログラム1430は、入力された問い合わせコードが正しい場合に、個人情報通知データを出力すると共に、入力された問い合わせコードに対応するレコードを問い合わせコード管理テーブル1520から削除するので、特定の問い合わせコードは個人情報参照者によって一度だけ使えるようになっていく。このため、個人情報参照者が個人情報を取得した後で問い合わせコードが第三者に漏洩してしまったとしても、その問い合わせコードを利用される恐れはない。

【0094】以上説明した本実施例によれば、本発明が解決しようとする2つの課題が解決される。すなわち、

(1) 個人情報登録者が指定する特定の個人情報参照者に対してのみ、個人情報をオンラインで取得させることが可能である。

【0095】(2) 個人情報登録者と、上記の特定の個人情報参照者との間で、電子化されたデータを授受する必要がない。

【0096】《第二の実施例》第一の実施例では、有効な登録者IDと問い合わせコードの組み合わせを知ることさえできれば、誰にでも個人情報を出力させることができってしまうので、発行された問い合わせコードを第三者から秘匿しなければならないという問題があった。

【0097】本実施例は上記の問題を解決することを目的としており、問い合わせコードが第三者に知られただけでは個人情報を無断に参照されることがないようにしている。すなわち、問い合わせコード発行処理において、個人情報登録者に、個人情報参照者を指定させるようにし、個人情報出力処理においては、端末装置20を操作する個人情報参照者が、個人情報登録者が指定した個人情報参照者本人であるかを確認した上で個人情報を出力するようにしている。

10 【0098】以下では、図面を用いて本実施例を詳細に説明する。本実施例は第一の実施例の構成を基本として構成しているので、第一の実施例との相違点について説明する。

【0099】図18は、本実施例における問い合わせコード発行申請画面620aの構成図である。問い合わせコード発行申請画面620aは、問い合わせコード発行申請画面620に、個人情報を参照させる個人情報参照者を指定するための参照者ID入力フィールド6203を追加した画面である。

20 【0100】図19は、本実施例における個人情報出力申請画面630aの構成図である。個人情報出力申請画面630aは、個人情報出力申請画面630に、端末装置20を操作している個人情報参照者の参照者IDと参照者パスワードをそれぞれ入力するための参照者ID入力フィールド6303と参照者パスワード入力フィールド6304を追加した画面である。

30 【0101】図20は、本実施例で二次記憶装置150上に設ける参照者管理テーブル1540の構成図である。参照者管理テーブル1540は、個人情報参照者を認証するために、参照者IDと参照者パスワードを対応づけるテーブルであり、参照者IDフィールド1541と参照者パスワードフィールド1542とを有する。

【0102】図21は、本実施例で二次記憶装置150上に設ける参照者指定テーブル1550の構成図である。参照者指定テーブル1550は、登録者IDと問い合わせコードの組を参照者IDと対応づけて記憶するためのテーブルであり、登録者IDフィールド1551と、問い合わせコードフィールド1552と参照者IDフィールド1553とを有する。

40 【0103】次に、本実施例における問い合わせコード発行処理について説明する。本実施例では、個人情報登録者に、個人情報を参照させる個人情報参照者の参照者IDを入力させ、発行する問い合わせコードに対応させてかかる参照者IDを記録しておくようにしている。

50 【0104】図22は、本実施例における問い合わせコード発行プログラム1420aの処理内容を示したPAD図である。問い合わせコード発行プログラム1420aは、第一の実施例における問い合わせコード発行プログラム1420に、以下の各ステップを追加することにより、問い合わせコードに対応づけて参照者IDを記録する

ようにしたプログラムである。

【0105】（ステップ50601）問い合わせコード発行プログラム1420aは、入力された参照者ID6203をワークエリア1440に格納する。

【0106】（ステップ50602）問い合わせコード発行プログラム1420aは、参照者記録ルーチン14230を呼び出して、問い合わせコードに対応づけて参照者ID6203を記録する。

【0107】図23は、問い合わせコード発行プログラム1420aが呼び出すサブルーチンである参照者記録ルーチン14230の処理内容を示すPAD図である。参照者記録ルーチン14230は、ワークエリア1440上に格納された登録者ID6201と、生成された問い合わせコードと、参照者ID6203を入力して、以下のステップにより、問い合わせコードに対応させて参照者IDを記録する。

【0108】（ステップ50701）参照者記録ルーチン14230は、登録者ID6201、生成した問い合わせコード、参照者ID6203の組をレコードとして参照者指定テーブル1550に追加する。

【0109】以上説明した問い合わせコード発行プログラム1420aと参照者記録ルーチン14230により、問い合わせコード発行処理において、個人情報登録者が指定した個人情報参照者の参照者IDが参照者指定テーブル1550に記録される。

【0110】次に、本実施例における個人情報出力処理について説明する。本実施例では個人情報を出力する際に個人情報参照者に参照者IDと参照者パスワードを入力させ、参照者パスワードを照合することにより個人情報参照者が本人であることを確認し、さらに問い合わせコードに対応して記録されている参照者IDと入力された参照者IDが一致する場合にのみ個人情報を出力するようにしている。

【0111】図24は、本実施例における個人情報出力プログラム1430aの処理内容を示したPAD図である。個人情報出力プログラム1430aは、第一の実施例における個人情報出力プログラム1430に、以下の各ステップを追加することにより、個人情報参照者の認証と、問い合わせコードと個人情報参照者の対応の確認をするようにしている。

【0112】（ステップ50801）個人情報出力プログラム1430aは、入力された参照者ID6303と参照者パスワード6304をワークエリア1450に格納する。

【0113】（ステップ50802）個人情報出力プログラム1430aは、参照者認証ルーチン14330を呼び出して、参照者ID6303と参照者パスワード6304を照合し、戻り値として照合の結果を示す論理値を得る。

【0114】（ステップ50803）個人情報出力プロ

グラム1430aは、上記戻り値がFALSE、すなわち参照者パスワード6304が不正であった場合には図示しないエラー通知画面に対応するエラー通知データを通信制御プログラム1410に出力して終了する（ステップ50804）。

【0115】（ステップ50805）個人情報出力プログラム1430aは、参照者一致検査ルーチン14340を呼び出して、参照者ID6303と問い合わせコード6302を照合し、戻り値として照合の結果を表す論理値を得る。

【0116】（ステップ50806）個人情報出力プログラム1430aは、参照者一致検査ルーチン14340の戻り値がFALSE、すなわち参照者ID6303が指定以外の参照者IDであった場合には、図示しないエラー通知画面に対応するエラー通知データを通信制御プログラム1410に出力して終了する（ステップ50807）。

【0117】以上のステップを追加することにより、個人情報出力プログラム1430aは入力された参照者パスワード6304が正しく、かつ参照者ID6303と問い合わせコード6302が対応する場合に限って個人情報を出力するようになる。

【0118】次に、個人情報出力プログラム1430aのサブルーチンとして本実施例で設ける参照者認証ルーチン14330と、参照者一致検査ルーチン14340の処理内容について説明する。

【0119】まず一つ目のサブルーチンである参照者認証ルーチン14330について説明する。参照者認証ルーチン14330は、ワークエリア1450上の参照者ID6303と参照者パスワード6304の対応を照合し、参照者パスワード6304が正しければTRUEを、正しくなければFALSEを返す。以下に、参照者認証ルーチン14330の処理内容を図25に示すPAD図に従って説明する。

【0120】（ステップ50901）参照者認証ルーチン14330は、参照者ID6303をキーとして参照者管理テーブル1540のレコードを検索する。

【0121】（ステップ50902）参照者認証ルーチン14330は、上記のレコードが存在し、かかるレコードの参照者パスワードフィールド1542と入力された参照者パスワード6304が一致する場合には、参照者パスワード6304が正しいことを意味するTRUEを返し（ステップ50903）、一致しない場合には正しくないことを意味するFALSEを返す（ステップ50904）。

【0122】次に、二つ目のサブルーチンである参照者一致検査ルーチン14340について説明する。参照者一致検査ルーチン14340は、ワークエリア1450上の参照者ID6301と問い合わせコード6302の対応を照合し、問い合わせコード6302が参照者ID63

10

20

30

40

50

01に対応すればTRUEを返し、対応しなければFALSEを返す。以下に、参照者一致検査ルーチン14340の処理内容を図26に示すPAD図に従って説明する。

【0123】(ステップ51001)参照者一致検査ルーチン14340は、登録者ID6301と、問い合わせコード6302の組をキーとして参照者指定テーブル1550のレコードを検索する。

【0124】(ステップ51002)参照者一致検査ルーチン14340は、当該レコードの参照者IDフィールド1553の内容が、入力された参照者ID6303と一致した場合には、参照者ID6303が個人情報登録者によって指定された正しい参照者IDであることを意味するTRUEを返し(ステップ51003)、一致しなかった場合には指定外の参照者IDであることを意味するFALSEを返す(ステップ51004)。

【0125】次に、以上説明したように構成された本実施例の動作について、第一の実施例の動作との相違点を中心に説明する。本実施例では、問い合わせコードの発行処理において個人情報登録者は問い合わせコード発行画面620aにおいて登録者ID6201と登録者パスワード6203に加えて、個人情報を参照させる個人情報参照者の参照者ID6203を入力する。ここで入力した参照者ID6203は、問い合わせコードの発行処理の過程で参照者記録ルーチン14230により、登録者ID6201と生成した問い合わせコードと対応づけて参照者指定テーブル1540に記録される。一方、個人情報出力処理においては、個人情報参照者は個人情報取得申請画面630aにおいて登録者ID6301と問い合わせコード6302の他に、自身の参照者ID6303と参照者パスワード6304を入力する。個人情報出力プログラム1430aは、まず参照者認証ルーチン14330によって参照者ID6303と参照者パスワード6304が対応が照合され、さらに参照者一致検査ルーチン14340によって参照者ID6303と登録者ID6301と問い合わせコード6302の対応が照合された後に始めて個人情報を出力する。すなわち、個人情報登録者が問い合わせコードの発行を受けるときに参照者ID6203で指定した個人情報参照者本人が操作した場合に限り、個人情報を出力させることが可能である。そのため、問い合わせコード自体は、第三者に知られてしまってもかまわない。

【0126】以上説明したように、本実施例によれば、発行された問い合わせコードを、個人情報を参照させたいと思う個人情報参照者以外の第三者に知られないように注意する必要性をなくすることが可能となっている。

【0127】《第三の実施例》第一または第二の実施例では、個人情報出力プログラム1430または1430aは個人情報を一回出力すると対応する問い合わせコードを問い合わせコード管理テーブル1520から削除するの

で、一度しか問い合わせコードを使用できない。そのため、一旦個人情報を参照した後で、個人情報の登録内容に変更があった場合などに、再び個人情報を参照しようとした場合には、個人情報登録者に再び問い合わせコードを発行してもらう必要がある。本実施例ではこの問題を解決することを目的としており、問い合わせコードに有効期限を設け、有効期限内であれば何度でも個人情報を出力させることを可能にしている。

【0128】以下では、図面を用いて本実施例を詳細に説明する。

【0129】本実施例は、第一の実施例の構成を基本として構成しているが、第二の実施例を基本として同様に構成することが可能である。

【0130】図27は、本実施例において二次記憶装置150上に追加する有効期限管理テーブル1560の構成図である。本テーブルは発行された問い合わせコードの有効期限を記録するためのテーブルであり、登録者IDフィールド1561と、問い合わせコードフィールド1562と、問い合わせコードの有効期限を記録する有効期限フィールド1563とを有する。本テーブルには問い合わせコードの発行処理の過程で問い合わせコードの有効期限が記録され、個人情報出力処理の過程で入力された問い合わせコードが有効期限を超過しているかどうかを検査される。

【0131】図28は、本実施例における個人情報出力プログラム1420bの処理内容を示したPAD図である。個人情報出力プログラム1420bは、第一の実施例における個人情報出力プログラム1420に、以下の各ステップを追加することにより、発行する問い合わせコードの有効期限を記録するようにしたプログラムである。

【0132】(ステップ51101)個人情報出力プログラム1420bは、有効期限記録ルーチン14240を呼び出して、問い合わせコードの有効期限を記録する。

【0133】図29は、個人情報出力プログラム1420bが呼び出すサブルーチンである有効期限記録ルーチン14240の処理内容を示したPAD図である。本ルーチンは、生成した問い合わせコードの有効期限を有効期限管理テーブル1560に記録するルーチンであり、以下のステップを有する。

【0134】(ステップ51201)有効期限管理テーブル1560は、登録者ID6201と生成した問い合わせコードと所定の有効期限の組をレコードとして、有効期限管理テーブル1560に追加する。

【0135】図31は、本実施例における問い合わせコード検定ルーチン14310aの処理内容を示したPAD図である。本ルーチンは、問い合わせコード検定ルーチン14310の処理内容に、有効期限の判定処理を加えたルーチンであり、問い合わせコード検定ルーチン14310に以下の各ステップを追加している。

【0136】(ステップ52401) 問い合わせコード検  
定ルーチン14310aは、参照者ID6301と問  
い合せコード6302をキーとして有効期限管理テーブル  
1563を検索する。

【0137】(ステップ52402) 問い合わせコード検  
定ルーチン14310aは、検索したレコードの有効期  
限フィールド1563が現時刻以前の時刻である、すな  
わち問い合わせコードの有効期限が超過している場合には  
ステップ50504～52404を実行する。

【0138】(ステップ52403) 問い合わせコード検  
定ルーチン14310aは、有効期限管理テーブル15  
60から上記レコードを削除する。

【0139】(ステップ52404) 問い合わせコード検  
定ルーチン14310aは、FALSEを返す。

【0140】以上の処理により、問い合わせコード管理テ  
ーブル1530のレコードは有効期限を過ぎた場合に始  
めて削除されるようになる。

【0141】以上説明した本実施例の構成によれば、所  
定の有効期限内であれば何度でも個人情報を出力する  
ことが可能である。

【0142】《第四の実施例》第一～第三の実施例で  
は、個人情報参照者が入力する問い合わせコードが、正規  
の問い合わせコード発行処理によって発行された問い合  
せコードであるかどうかを検定する方法として、問い合せ  
コードの発行時に問い合わせコード管理テーブルに記録し  
ていた問い合わせコードと個人情報参照者が入力した問い  
合せコードを照合する方法をとっていた。そのため、問  
い合せコードを発行するたびに問い合わせコード管理  
テーブルにレコードを追加していく必要があり、問い合  
せコード発行処理の回数に比例して問い合わせコード管理  
テーブルの容量が増加してしまうという問題があった。

【0143】本実施例は上記の問題を解決することを目  
的とし、発行する個々の問い合わせコードに対応した情報  
を記録する必要をなくしている。本実施例では、暗号技  
術を応用した問い合わせコード生成方法を用いることによ  
り、発行する個々の問い合わせコードに対応したレコード  
を記録することなしに、個人情報参照者が入力する問い  
合せコードを検定することを可能にしている。

【0144】まず、本実施例の原理について説明する。

【0145】本実施例では、問い合わせコード発行処理に  
おいて、個人情報登録者が入力した登録者と参照者ID  
の関数として問い合わせコードを生成する。ここで用いる  
関数である問い合わせコード生成関数の関数式は利用者  
には非公開であり、登録者IDと参照者IDを元に利用  
者が正規の問い合わせコード発行処理によらずに独自に  
問い合わせコードを算出することができないようになっ  
ている。

【0146】一方の個人情報出力処理では、個人情報参  
照者に、登録者IDと参照者IDと問い合わせコードを入  
力させ、入力された登録者IDと参照者IDを元に問い

合せコードを再計算し、入力された問い合わせコードと再  
計算した問い合わせコードとを照合する。入力された問  
い合せコードと再計算した問い合わせコードが一致すれば、  
入力された問い合わせコードは正規の問い合わせコード発行  
処理によって得られたコードであるとみなすことができ  
る。

【0147】ここでもしもある個人情報参照者が、個人  
情報登録者に無断で個人情報を出力させようとした場合  
には、かかる個人情報参照者は、かかる個人情報登録者  
の登録者IDと自身の参照者IDの組み合わせに対応す  
る問い合わせコードを入手しなければならない。ところ  
が、問い合わせコードの正規の入手方法である、問い合せ  
コード発行処理は、個人情報登録者の登録者パスワード  
を入力しなければ実行できないので、それを知らない、  
かかる個人情報参照者に問い合わせコード発行処理を実行  
させることはできない。他方、問い合わせコード発行処理  
を経ずに、問い合わせコードを独自に算出しようとして  
も、問い合わせコードを生成する関数式を知らない限りそ  
れは不可能である。すなわち個人情報参照者が問い合せ  
コードを入手するには、個人情報の持ち主である個人情  
報登録者が正規の問い合わせコード発行処理によって問  
い合せコードを発行させた場合に限られる。

【0148】以上の原理を図を用いて説明する。

【0149】まず、図31に、本実施例における問い合  
せコード生成処理の原理図を示す。本実施例では、問い  
合せコード生成処理において、個人情報登録者が入力し  
た登録者ID6201と参照者ID6202を接続して  
二次記憶装置140に設ける平文領域1491に格納  
し、問い合わせコード生成関数を実装したルーチンである  
関数型問い合わせコード生成ルーチン1480を起動す  
る。関数型問い合わせコード生成ルーチン1480は平文  
領域1491の内容の関数として問い合わせコード149  
2を計算して出力する。このように生成された問い合せ  
コード1492は個人情報登録者に出力される。

【0150】次に、図32に、本実施例における問い合  
せコード検定処理の原理図を示す。本実施例では問い合  
せコード検定処理において、個人情報参照者が入力した  
登録者ID6301と参照者ID6303を接続して平  
文領域1491に格納し、関数型問い合わせコード生成ル  
ーチン1480を起動する。関数型問い合わせコード生成  
ルーチン1480は平文領域1491の内容の関数とし  
て問い合わせコード1492を計算して出力する。次に、  
計算した問い合わせコード1492と個人情報参照者が入  
力した問い合わせコード6302とを比較し、両者が一致  
したら正規の問い合わせコードが入力されたとみなす。

【0151】次に、本実施例の構成について説明する。

【0152】本実施例は第二の実施例の構成を基本とし  
ており、二次記憶装置上に格納するテーブルの構造と、  
プログラムの処理内容が異なる。以下に第二の実施例と  
の相違点について説明する。



【0153】本実施例における端末装置の表示や利用者の操作方法は第二の実施例と同一である。すなわち、個人情報登録者は個人情報参照者を指定して問い合わせコード発行処理を指示し、個人情報参照者は自身の参照者IDと参照者パスワードを入力した上で個人情報を取得する。

【0154】図33は、本実施例で二次記憶装置150に格納する情報の構成図である。二次記憶装置150には、第二の実施例で設けていた個人情報テーブル1510と、登録者管理テーブル1530と画面データファイル群1590と、本実施例において新たに設ける秘密鍵ファイル1570を格納する。秘密鍵ファイルは問い合わせコード生成関数がパラメータとして用いるデータを格納したファイルである。

【0155】図34は、秘密鍵ファイル1570の構成図である。秘密鍵ファイル1570は、関数型問い合わせコード生成ルーチン1480が使用するパラメータである秘密鍵データ1571を格納している。秘密鍵データ1571には、装置の運用に先立って乱数により生成した値を格納しておき、その具体的な値は利用者には公開しないでおく。

【0156】図35は、本実施例における問い合わせコード発行プログラム1420cの処理内容を示したPAD図である。問い合わせコード発行プログラム1420cは、第二の実施例における問い合わせコード発行プログラム1420aに置き換えて設けるルーチンであり、以下のステップを有する。

【0157】（ステップ51501）問い合わせコード発行プログラム1420cは、入力された登録者ID6201、登録者パスワード6202、参照者ID6203をワークエリア1440に格納する。

【0158】（ステップ51502）問い合わせコード発行プログラム1420cは、個人情報参照者認証ルーチン14210を呼び出して、登録者ID6201と登録者パスワード6202を照合する。

【0159】（ステップ51503）問い合わせコード発行プログラム1420cは、個人情報参照者認証ルーチン14210の戻り値がTRUE、すなわちパスワードが正しければステップ51504～51506を、戻り値がFALSE、すなわちパスワードが正しくなければステップ51507を実行する。

【0160】（ステップ51504）問い合わせコード発行プログラム1420cは、登録者ID6201と、参照者ID6203を接続して平文領域1491に格納する。

【0161】（ステップ51505）問い合わせコード発行プログラム1420cは、関数型問い合わせコード生成ルーチン1480を呼び出して、問い合わせコードを生成する。

【0162】（ステップ51506）問い合わせコード発

行プログラム1420cは、関数型問い合わせコード生成ルーチン1480の戻り値の問い合わせコードを元に、問い合わせコード通知画面640に対応する問い合わせコード通知データを生成して通信制御プログラム1410に出力する。

【0163】（ステップ51507）問い合わせコード発行プログラム1420cは、パスワードが不正であった旨を伝えるエラー通知データを通信制御プログラム1410に出力して終了する。

10 【0164】以上の処理により、問い合わせコードは個人情報登録者が登録者IDとそれに対応する正しい登録者パスワードを入力した場合に限り発行される。ここで発行される問い合わせコードは個人情報登録者が入力した登録者IDと参照者IDの組の関数として計算される。

【0165】図36は、本実施例における個人情報出力プログラム1430bの処理内容を示したPAD図である。本プログラムは、第二の実施例における個人情報出力プログラム1430に置き換えて設けるプログラムであり、以下のステップを有する。

20 【0166】（ステップ51601）個人情報出力プログラム1430bは、入力された登録者ID6301と、問い合わせコード6302と、参照者ID6303と参照者パスワード6304をワークエリア1450に格納する。

【0167】（ステップ51602）個人情報出力プログラム1430bは、参照者認証ルーチン14330を呼び出して、参照者ID6303と参照者パスワード6304を照合して、戻り値として照合の結果を示す論理値を得る。

30 【0168】（ステップ51603）個人情報出力プログラム1430bは、参照者認証ルーチン14330の戻り値がFALSE、すなわち参照者パスワードが不正であった場合にはパスワードが不正である旨を告げるエラー通知データを通信制御プログラム1410に出力して終了する（ステップ51604）（ステップ51605）個人情報出力プログラム1430bは、登録者ID6301と参照者ID6303を接続して平文領域1491に格納する。

40 【0169】（ステップ51606）個人情報出力プログラム1430bは、関数型問い合わせコード検定ルーチン14350を呼び出して問い合わせコード6302を照合し、照合結果を示す論理値を戻り値として得る。

【0170】（ステップ51607）個人情報出力プログラム1430bは、関数型問い合わせコード検定ルーチン14350の戻り値がFALSE、すなわち問い合わせコードが不正であった場合には問い合わせコードが不正である旨を告げるエラー通知データを通信制御プログラム1410に出力して終了する（ステップ51608）。

50 【0171】（ステップ51609）個人情報出力プログラム1430bは、個人情報テーブル1510から登

録者 I D 6 3 0 1 に対応するレコードを読み出し、ワークエリア 1 4 5 0 に格納する。

【0 1 7 2】（ステップ 5 1 6 1 0）個人情報出力プログラム 1 4 3 0 b は、読み出したレコードの内容を個人情報通知画面 6 5 0 に対応する個人情報通知データに変換して通信制御プログラム 1 4 1 0 に出力する。

【0 1 7 3】以上の処理により、個人情報参照者が入力した参照者 I D と参照者パスワードが対応し、さらに登録者 I D と参照者 I D の組み合わせが、個人情報参照者が入力した問い合わせコードに対応した場合に限り、入力された登録者 I D に関する個人情報が出力される。すなわち、個人情報出力処理を実行させることができるのは参照者パスワードを知っている個人情報参照者本人であり、さらにかかる個人情報参照者は問い合わせコード発行処理において個人情報登録者が参照者 I D によって指定した個人情報参照者である場合に限られる。

【0 1 7 4】図 3 7 は、本実施例において主記憶装置 1 4 0 に設ける関数型問い合わせコード生成ルーチン 1 4 8 0 の処理内容を示した P A D 図である。関数型問い合わせコード生成ルーチン 1 4 8 0 は、問い合わせコード生成関数を実装したルーチンであり、主記憶装置 1 4 0 に設ける平文領域 1 4 9 1 に格納されたデータから問い合わせコードを関数式によって求めて出力する。

【0 1 7 5】本実施例では問い合わせコードを算出する関数式の一例として、暗号アルゴリズムの一種として提案されているメッセージダイジェスト関数を応用した関数式を用いる。メッセージダイジェスト関数は、前掲書の p. 218 に紹介されているように、可変長の、典型的には長大な入力データに対して固定長の短いダイジェストデータを出力する関数であり、入力データの僅かな差異が出力データの大きな変化となって現れることを特徴としている。そのため、データの改竄を受ける危険性のある伝送路を用いてデータを送信する場合に送信対象データの改竄の検出に用いられている。メッセージダイジェスト関数の具体的な関数式としてはダイジェストデータの長さや計算量の異なる各種の関数が提案されているが、本実施例では出力されるダイジェストデータの長さが、人手によって書き移すのに不自由のない長さになれば、どのような関数式を用いてもかまわない。

【0 1 7 6】本実施例では平文領域 1 4 9 1 に、利用者には非公開のデータである秘密鍵データ 1 5 7 1 を追加してからメッセージダイジェスト関数を適用するようにしている。これにより、本ルーチン全体としての関数式は利用者には非公開の関数式になる。すなわち、本ルーチンの処理内容が第三者に知られた場合であっても秘密鍵データ 1 5 7 1 の具体的な値を知ること無しに、第三者は本ルーチンに代って独自に問い合わせコードを計算することは不可能である。

【0 1 7 7】関数型問い合わせコード生成ルーチン 1 4 8 0 の処理の各ステップを図 3 7 に従って説明する。

【0 1 7 8】（ステップ 5 1 7 0 1）関数型問い合わせコード生成ルーチン 1 4 8 0 は、平文領域 1 4 9 1 に秘密鍵データ 1 5 7 1 を追加する。

【0 1 7 9】（ステップ 5 1 7 0 2）関数型問い合わせコード生成ルーチン 1 4 8 0 は、平文領域 1 4 9 1 のメッセージダイジェストを計算して問い合わせコードとする。

【0 1 8 0】（ステップ 5 1 7 0 2）関数型問い合わせコード生成ルーチン 1 4 8 0 は、計算した問い合わせコードを戻り値として返す。

10 【0 1 8 1】以上の処理により、平文領域 1 4 9 1 に格納された登録者 I D と参照者 I D の関数として問い合わせコードが生成される。

【0 1 8 2】図 3 8 は、本実施例において設ける関数型問い合わせコード検定ルーチン 1 4 3 5 0 の処理内容を示す P A D 図である。関数型問い合わせコード検定ルーチン 1 4 3 5 0 は、個人情報出力プログラム 1 4 3 0 b から呼び出され、個人情報参照者が入力し、個人情報出力プログラムが平文領域 1 4 9 1 に格納したデータから問い合わせコードを計算し、計算された問い合わせコードと個人情報参照者が入力した問い合わせコードを照合することによって問い合わせコードの検定を行うルーチンである。本ルーチンは以下のステップを有する。

20 【0 1 8 3】（ステップ 5 1 8 0 1）関数型問い合わせコード検定ルーチン 1 4 3 5 0 は、関数型問い合わせコード生成ルーチン 1 4 8 0 を呼び出して、入力されたデータから問い合わせコードを計算する。

【0 1 8 4】（ステップ 5 1 8 0 2）関数型問い合わせコード検定ルーチン 1 4 3 5 0 は、計算した問い合わせコードと入力された問い合わせコード 6 3 0 2 が一致する、すなわち入力された問い合わせコードが正しければ T R U E を返し（ステップ 5 1 8 0 3）、両者が一致しない、すなわち入力された問い合わせコードが誤っていれば F A L S E を返す（ステップ 5 1 8 0 4）。

【0 1 8 5】以上の処理により、個人情報参照者が入力した登録者 I D と参照者 I D が、個人情報参照者が入力した問い合わせコードと対応する場合にのみ、本ルーチンは問い合わせコードの検定が成功したことを意味する T R U E を返す。

【0 1 8 6】以上説明したように、本実施例によれば、問い合わせコード発行処理の度に二次記憶装置上のテーブルにレコードを追加する必要をなくすることが可能となる。

【0 1 8 7】《第五の実施例》第四の実施例では、全ての問い合わせコード発行処理において共通の秘密鍵データ 1 5 7 1 を使用しているために、関数型問い合わせコード生成ルーチン 1 4 8 0 の処理内容と秘密鍵データ 1 5 7 1 の具体的な値が個人情報参照者に知られてしまった場合には、かかる個人情報参照者は任意の登録者 I D と自身の参照者 I D に対応する問い合わせコードを、独自に計算することができてしまう。その結果、かかる個人情報

参照者は任意の個人情報登録者に問い合わせコード発行処理を実行してもらわなくても、個人情報を取得できてしまうという問題がある。本実施例は上記の問題を解決することを目的としており、複数の秘密鍵データを用意し、登録者IDに応じてそれらの秘密鍵を使い分けることによっていずれかの秘密鍵データが知られてしまった場合であっても、それが直ちに全ての個人情報登録者に関する個人情報の漏洩につながらないようにしている。秘密鍵データは登録者IDと一対一で設けてもよいが、以下で説明する構成では、固定した数の秘密鍵データを設け、それぞれの秘密鍵データに秘密鍵IDを振り、登録者IDの関数によって秘密鍵IDを決定することにより、秘密鍵データの数を減らすようにしている。また、登録者IDから秘密鍵IDを決定する関数の例として本実施例では登録者IDの下三桁の数字を用いている。登録者IDから秘密鍵IDを決定する関数として他の関数式を用いることも可能である。

【0188】以下に、本実施例の構成を説明する。本実施例は第四の実施例を基本として構成されており、以下の要素が第四の実施例と異なる。

【0189】図39は本実施例において、二次記憶装置150に追加する秘密鍵テーブル1580の構成図である。秘密鍵テーブル1580は、秘密鍵IDと対応づけて複数の秘密鍵データを記憶するためのテーブルであり、秘密鍵IDフィールド1581と秘密鍵データフィールド1582を有する。

【0190】秘密鍵テーブル1580には、個人情報管理装置101の運用前に、“000”から“999”の間の1000通りの秘密鍵IDに対応してそれぞれ秘密鍵データを乱数によって生成して登録しておく。

【0191】図40は、第四の実施例における問い合わせコード生成ルーチン1480に置き換えて本実施例で設ける関数型問い合わせコード生成ルーチン1480aの処理内容を示したPAD図である。関数型問い合わせコード生成ルーチン1480aは、登録者IDに対応した秘密鍵データを秘密鍵テーブル1580から検索して問い合わせコードを生成するようにしている。本ルーチンの処理内容を図に従って説明する。

【0192】(ステップ52101) 関数型問い合わせコード生成ルーチン1480aは、平文領域1491に格納された登録者ID6201の下三桁を秘密鍵IDとする。

【0193】(ステップ52102) 関数型問い合わせコード生成ルーチン1480aは、算出した秘密鍵IDをキーとして秘密鍵管理テーブル1580を検索する。

【0194】(ステップ52103) 関数型問い合わせコード生成ルーチン1480aは、検索したレコードの秘密鍵フィールド1582の内容を、平文領域1491に追加する。

【0195】(ステップ52104) 関数型問い合わせコ

ード生成ルーチン1480aは、平文領域1491のメッセージダイジェストを計算して問い合わせコードとする。

【0196】(ステップ52105) 関数型問い合わせコード生成ルーチン1480aは、計算した問い合わせコードを返す。

【0197】以上の処理によれば、登録者IDに応じて異なった秘密鍵データが用いられるようになる。

【0198】《第六の実施例》第一〜第五の実施例では端末装置20として汎用の計算機を用い、個人情報管理装置10と端末装置20の間を通信網で接続した構成を示したが、その構成では本発明を利用しようとする個人情報登録者や個人情報参照者は通信網に接続された計算機を所有しなければならず、利用者が負担しなければならないコストが高いという問題がある。本実施例は、上記の問題点を解決して利用者が負担しなければならないコストを低減することを目的としており、端末として一般に普及しているプッシュホンやファクシミリ装置を利用している。

【0199】本実施例では第一〜第五の実施例において画面上の表示として利用者に出力していた操作案内や出力結果を音声ガイドやFAXの出力によって置き換えている。一方、利用者から装置への入力プッシュホンによる発信音による入力置き換えている。

【0200】図41は、本実施例のシステム構成図である。本実施例では個人情報管理装置10aは電話網30aを経由して、個人情報登録者が端末装置として利用するプッシュホン20aや、個人情報参照者が端末装置として利用するファクシミリ装置20bに接続されている。

【0201】図42は、本実施例における個人情報管理装置10aの構成図である。

【0202】本実施例における個人情報管理装置10aは、第一の実施例における個人情報管理装置10を基本として、以下の要素を置き換えて構成している。

【0203】まず、ネットワークインタフェース回路120に換えて、電話網30aに接続された電話回線インタフェース回路120aを設ける。電話回線インタフェース回路120aは、CPU110からの指示に従って電話の着信処理と、プッシュホンからの発信音の受信処理と、案内音声やFAXデータの送信処理を行う回路である。

【0204】次に、主記憶上の通信制御プログラム1410に換えて、音声・FAX応答型通信制御プログラム1410aを設ける。音声・FAX応答型通信制御プログラム1410aは、通信制御プログラム1410が端末装置20と送受信していたデータを以下の形式に置き換えて送受信するプログラムである。

【0205】(1) 操作の案内と、入力を促す画面データを出力する代わりに、その画面に相当する案内音声

を出力する。個人情報出力画面650のように情報量が多い画面に対しては、画面に表示すべきデータをFAXデータに変換して出力する。

【0206】(2) 利用者に画面上で処理を選択させたり、登録者IDなどのデータを入力させる代わりに、プッシュホンの発信音によってデータを入力させる。

【0207】上記の構成によれば、利用者は一般に普及しているプッシュホンやファクシミリ装置を端末装置として利用することができるので、利用者が負担すべきコストを低減することが可能である。

【0208】

【発明の効果】本発明によれば、住民票データや印鑑証明データを始めとする個人情報を管理し、個人情報の持ち主の要請によって個人情報データを出力する個人情報管理装置において、個人情報登録者が指定する特定の個人情報参照者に対してのみ、個人情報をオンラインで取得させることが可能となる。また、個人情報登録者と、上記の特定の個人情報参照者との間で、電子化されたデータを授受する必要をなくすることが可能となる。

【図面の簡単な説明】

【図1】第一の実施例のシステム構成図である。

【図2】個人情報管理装置10の構成図である。

【図3】二次記憶装置150の構成図である。

【図4】個人情報テーブル1510の構成図である。

【図5】問い合わせコード管理テーブル1520の構成図である。

【図6】登録者管理テーブル1530の構成図である。

【図7】画面データファイル群1590の構成図である。

【図8】処理選択画面610の構成図である。

【図9】問い合わせコード発行申請画面620の構成図である。

【図10】個人情報出力申請画面630の構成図である。

【図11】問い合わせコード通知画面640の構成図である。

【図12】個人情報通知画面650の構成図である。

【図13】問い合わせコード発行プログラム1420のPAD図である。

【図14】個人情報登録者認証ルーチン14210のPAD図である。

【図15】問い合わせコード生成ルーチン14220のPAD図である。

【図16】個人情報出力プログラム1430のPAD図である。

【図17】問い合わせコード検定ルーチン14310のPAD図である。

【図18】問い合わせコード発行申請画面620aの構成図である。

【図19】個人情報出力申請画面630aの構成図であ

る。

【図20】参照者管理テーブル1540の構成図である。

【図21】参照者指定テーブル1550の構成図である。

【図22】問い合わせコード発行プログラム1420aのPAD図である。

【図23】参照者記録ルーチン14230のPAD図である。

10 【図24】個人情報出力プログラム1430aのPAD図である。

【図25】個人情報参照者認証ルーチン14330のPAD図である。

【図26】参照者位置検査ルーチン14340のPAD図である。

【図27】有効期限管理テーブル1560の構成図である。

【図28】問い合わせコード発行プログラム1420bのPAD図である。

20 【図29】有効期限記録ルーチン14240のPAD図である。

【図30】問い合わせコード検定ルーチン14310aのPAD図である。

【図31】第四の実施例における問い合わせコードの生成方法の原理図である。

【図32】第四の実施例における問い合わせコードの検定方法の原理図である。

【図33】第四の実施例における二次記憶装置150の構成図である。

30 【図34】秘密鍵ファイル1570の構成図である。

【図35】問い合わせコード発行プログラム1420cのPAD図である。

【図36】個人情報出力プログラム1430bのPAD図である。

【図37】関数型問い合わせコード生成ルーチン1480のPAD図である。

【図38】関数型問い合わせコード検定ルーチン14350のPAD図である。

【図39】秘密鍵テーブル1580の構成図である。

40 【図40】関数型問い合わせコード生成ルーチン1480aのPAD図である。

【図41】第6の実施例のシステム構成図である。

【図42】個人情報管理装置10aの構成図である。

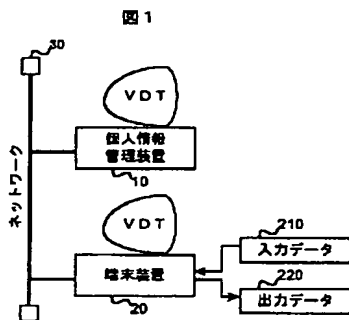
【図43】本発明の動作説明図である。

【符号の説明】

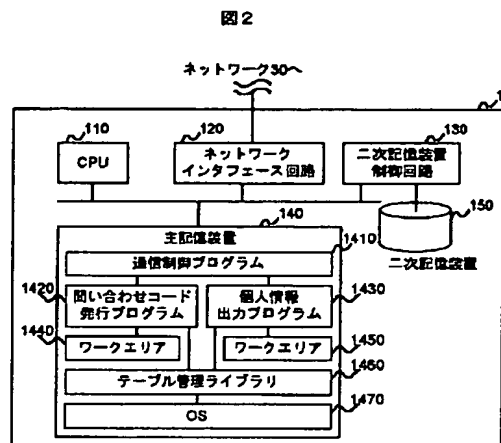
10…個人情報管理装置、20…端末装置、30…ネットワーク、110…CPU、120…ネットワークインタフェース回路、130…二次記憶装置制御回路、140…主記憶装置、150…二次記憶装置、230…契約書類、610…処理選択画面、620…問い合わせコード

発行申請画面、630…個人情報出力申請画面、640…問い合わせコード通知画面、650…個人情報通知画面、71…個人情報登録者、72…個人情報参照者、1410…通信制御プログラム、1420…問い合わせコード発行プログラム、1430…個人情報出力プログラム、1440…ワークエリア、1450…ワークエリア、1460…テーブル管理ライブラリ、1470…OS、1480…関数型問い合わせコード生成ルーチン、1510…個人情報テーブル、1520…問い合わせコード管理テーブル、1530…登録者管理テーブル、154 10

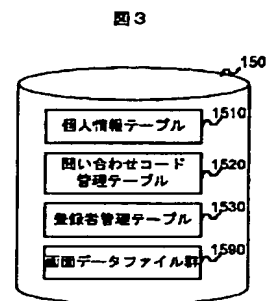
【図1】



【図2】



【図3】



【図4】

図4

登録者ID	住所	世帯主氏名	...
A1001	桜台50番地2号	田中一郎	
:	:	:	:

1510

【図5】

図5

登録者ID	問い合わせコード
A1001	589234
:	:

1520

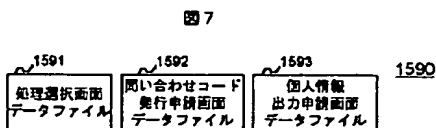
【図6】

図6

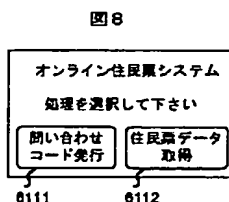
登録者ID	登録者パスワード
A1001	X9P21A
:	:

1530

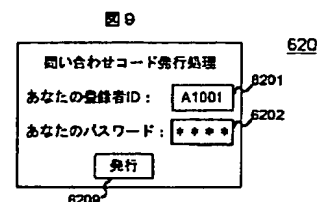
【図7】



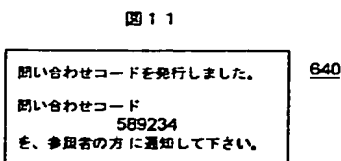
【図8】



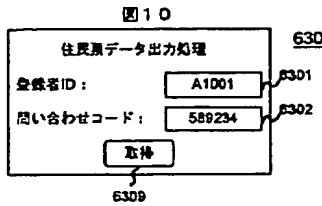
【図9】



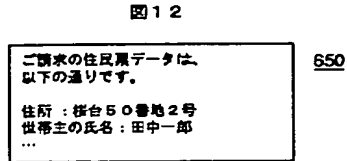
【図11】



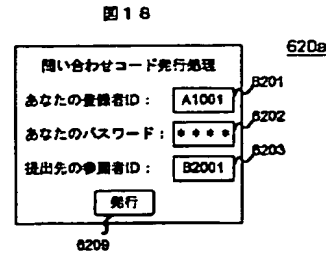
【図10】



【図12】

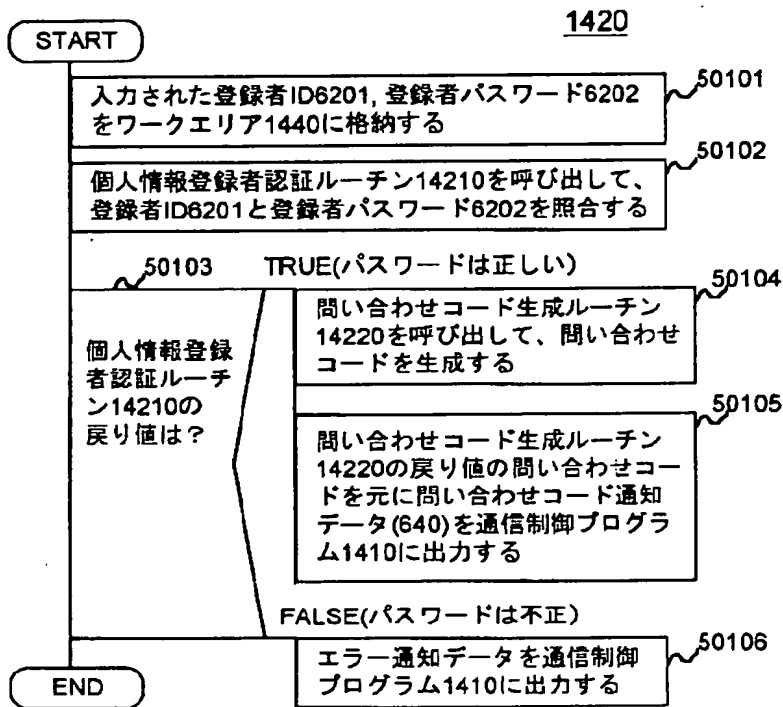


【図18】



【図13】

図13



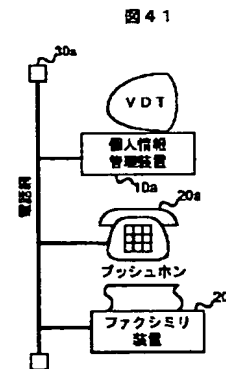
【図27】

図27

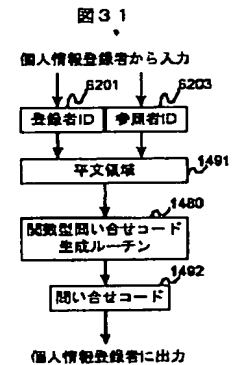
登録者ID	問い合わせコード	有効期限
A1001	589234	980331
:	:	:

1560

【図41】

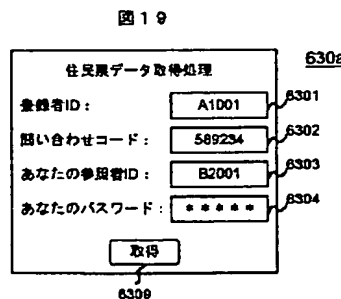


【図31】



【図33】

【図19】



【図20】

図20

参照者ID	参照者パスワード
B2001	551PCB
:	:

1540

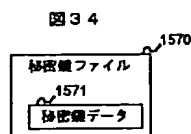
【図21】

図21

登録者ID	問い合わせコード	参照者ID
A1001	589234	B2001
:	:	:

1550

【図34】



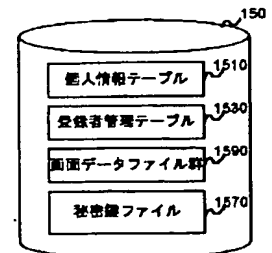
【図39】

図39

秘密鍵ID	秘密鍵
001	985762
:	:

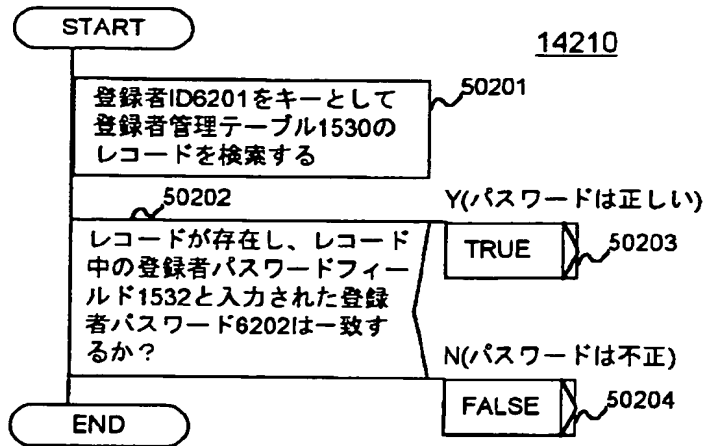
1580

図33



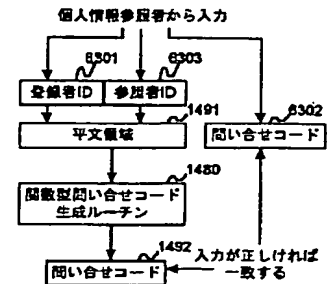
【図 14】

図 14



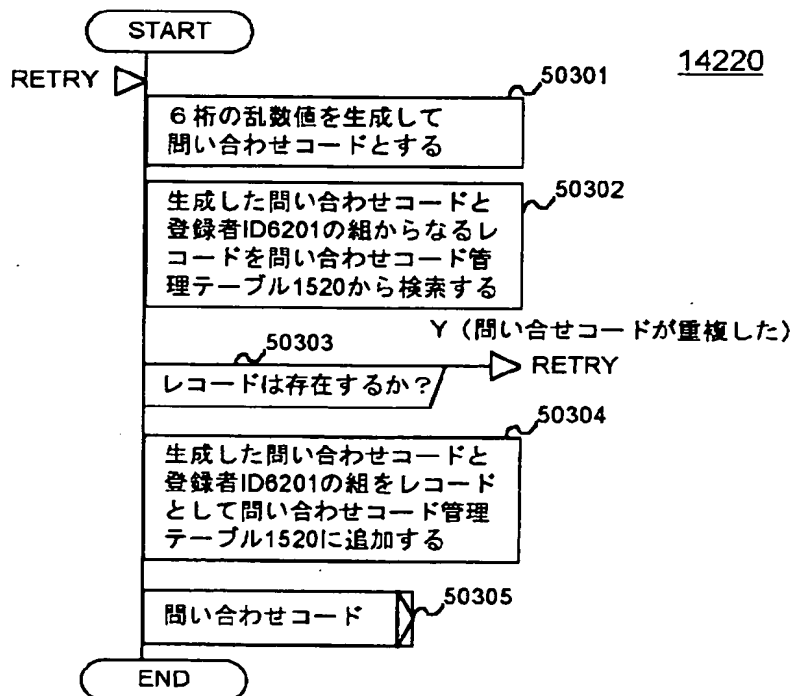
【図 32】

図 32



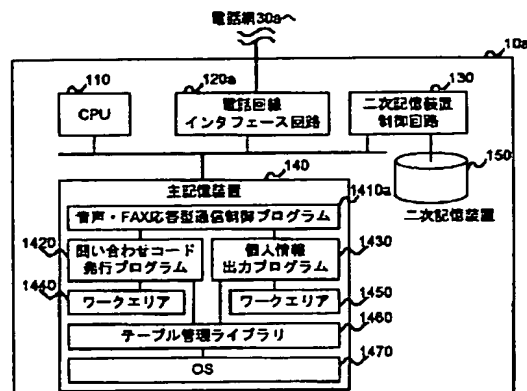
【図 15】

図 15



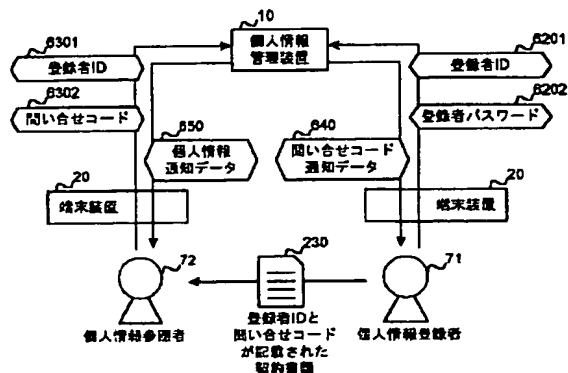
【圖 4 2】

42



【图 4 3】

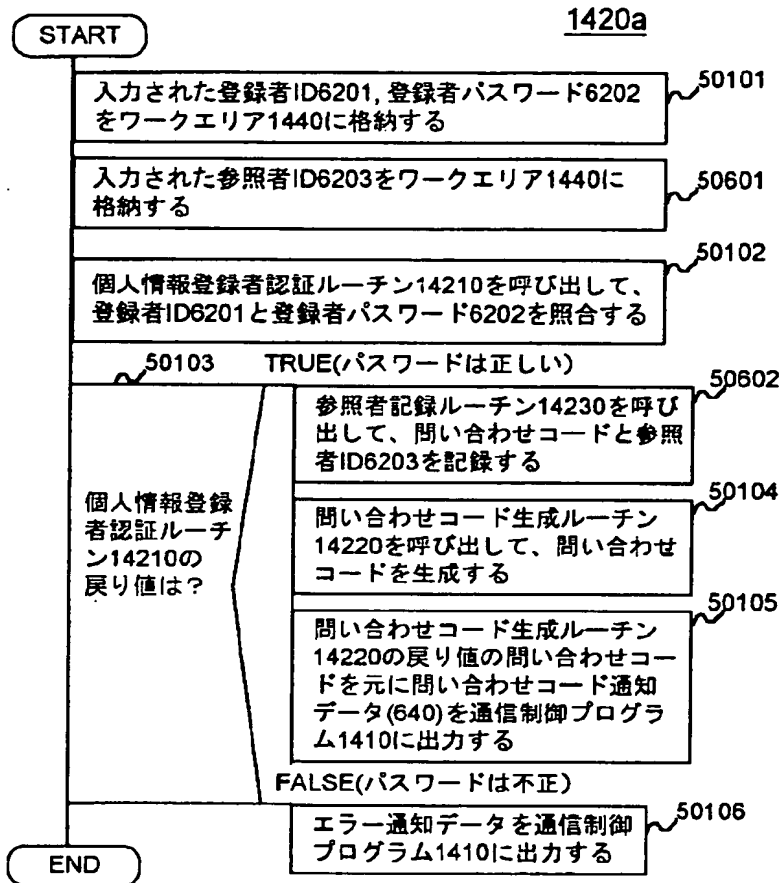
**图 4-3**





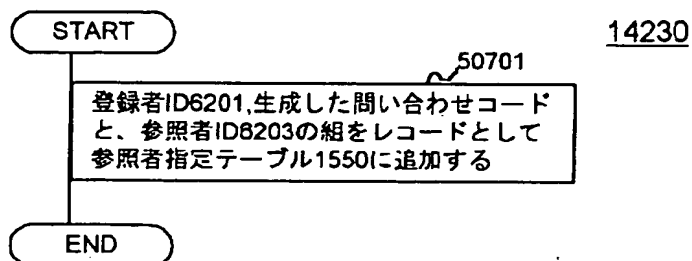
【図 22】

図 22



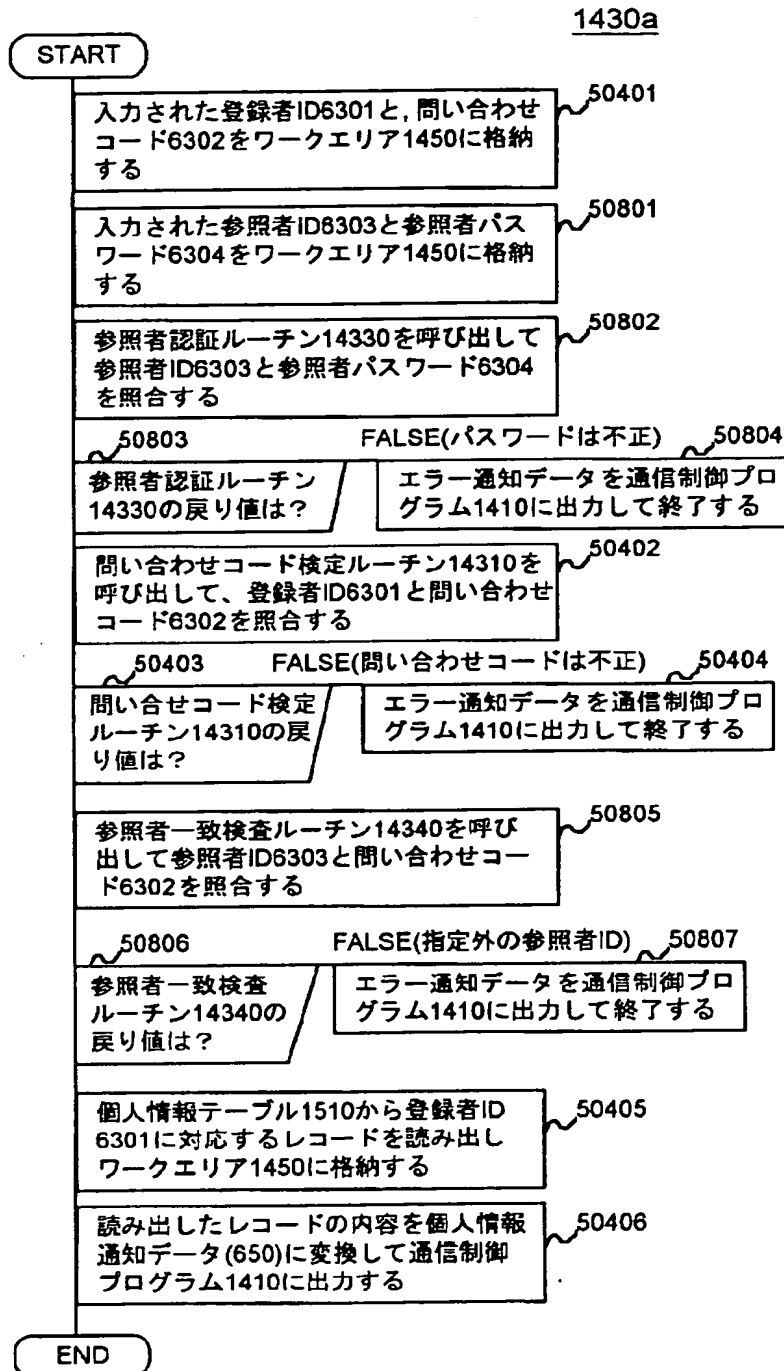
【図 23】

図 23



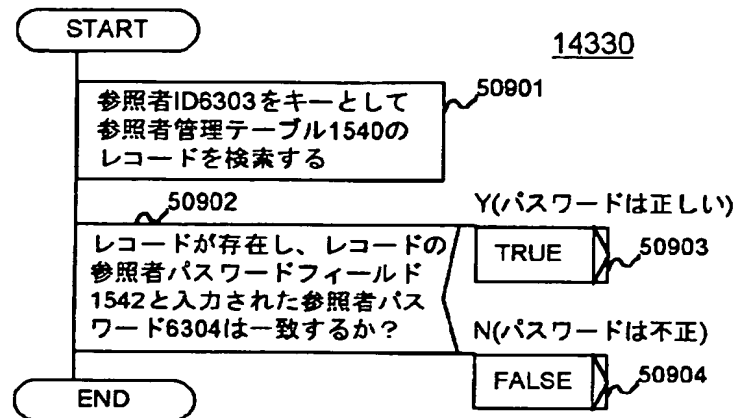
【図 2 4】

図 2 4



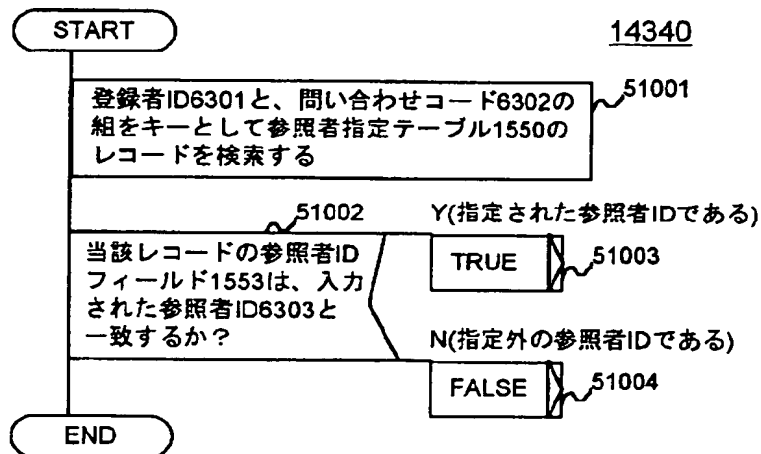
【図25】

図25



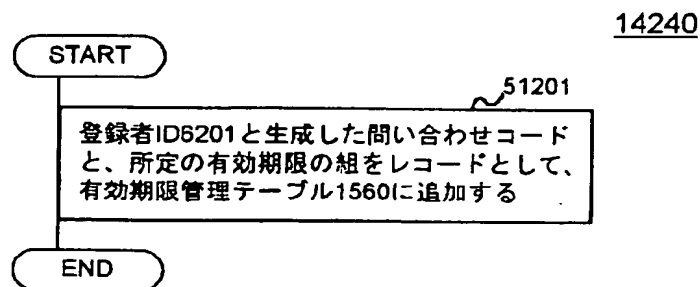
【図26】

図26



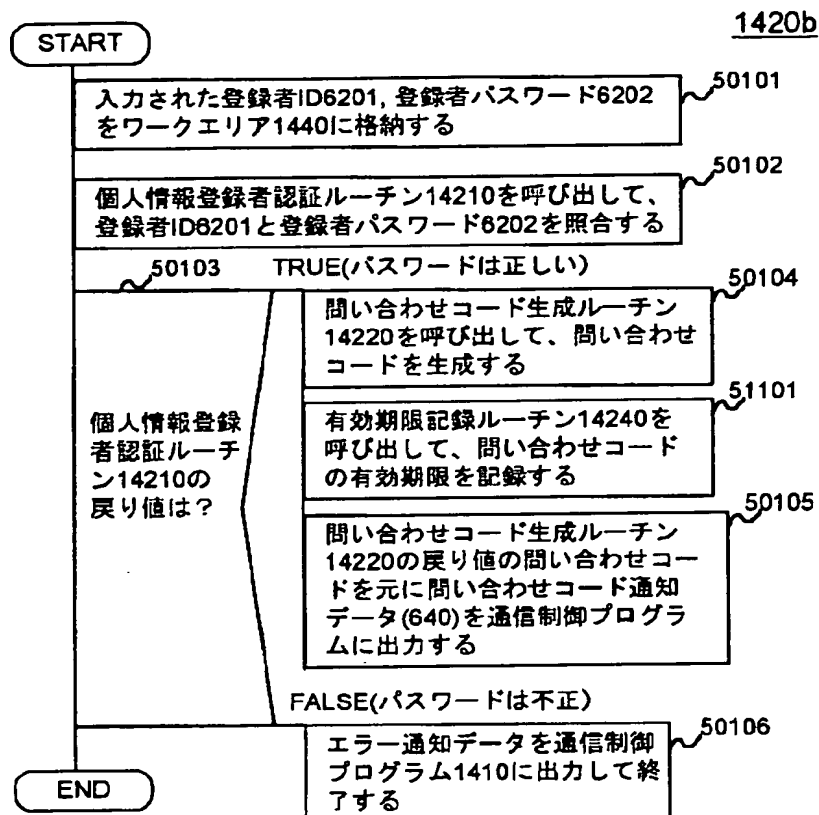
【図29】

図29



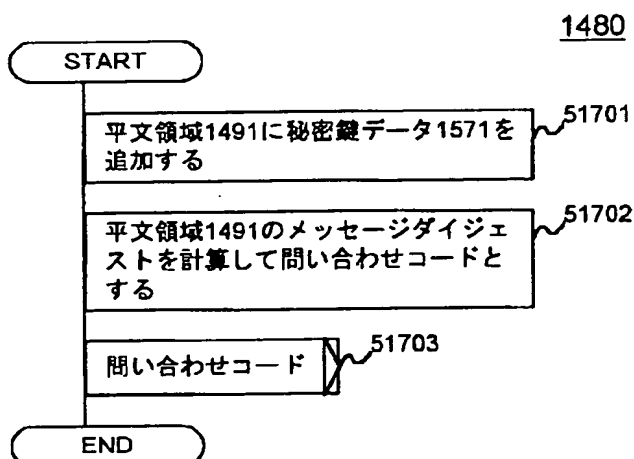
【図 2 8】

図 2 8



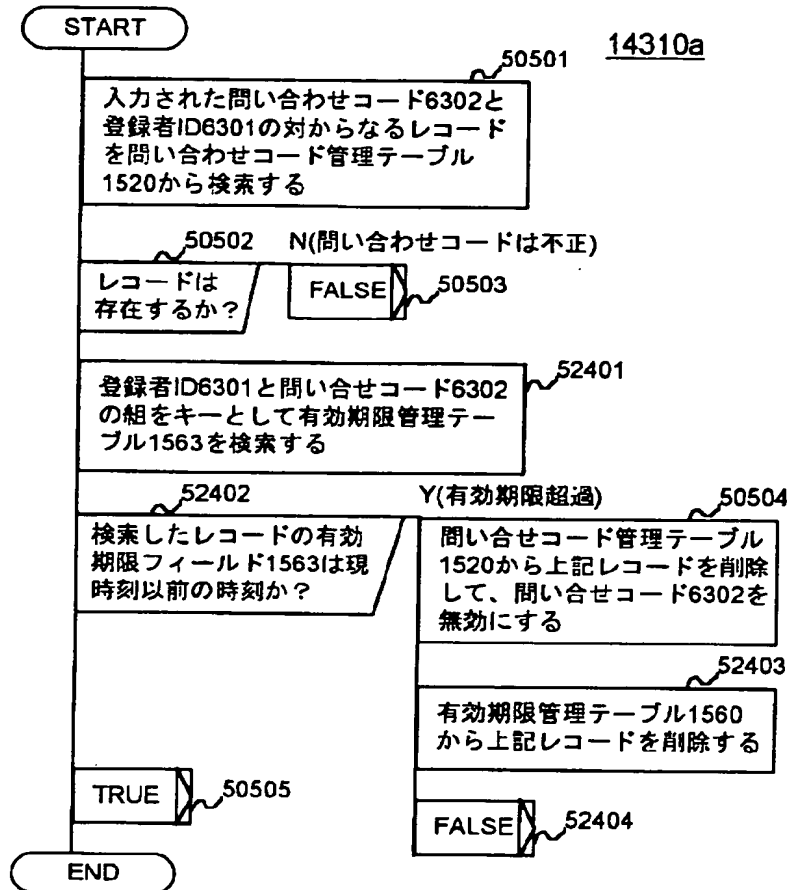
【図 3 7】

図 3 7



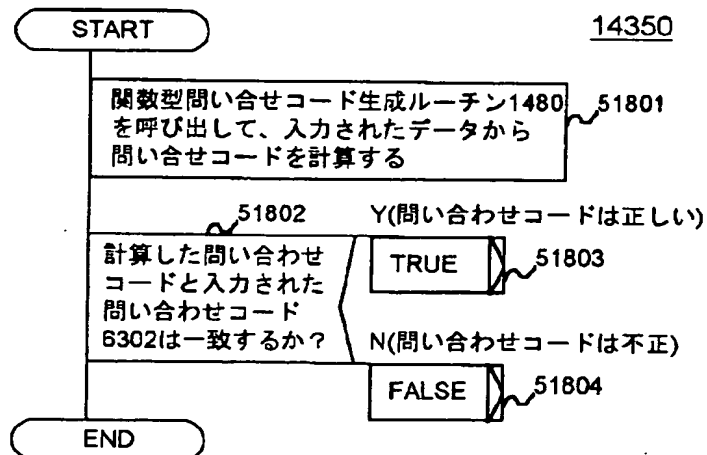
【図 30】

図 30



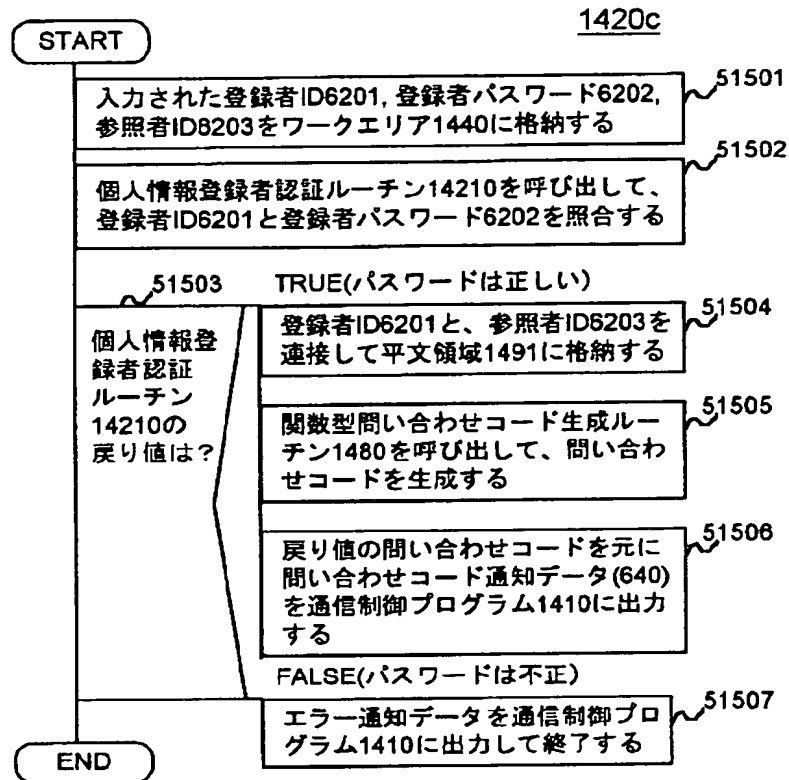
【図 38】

図 38



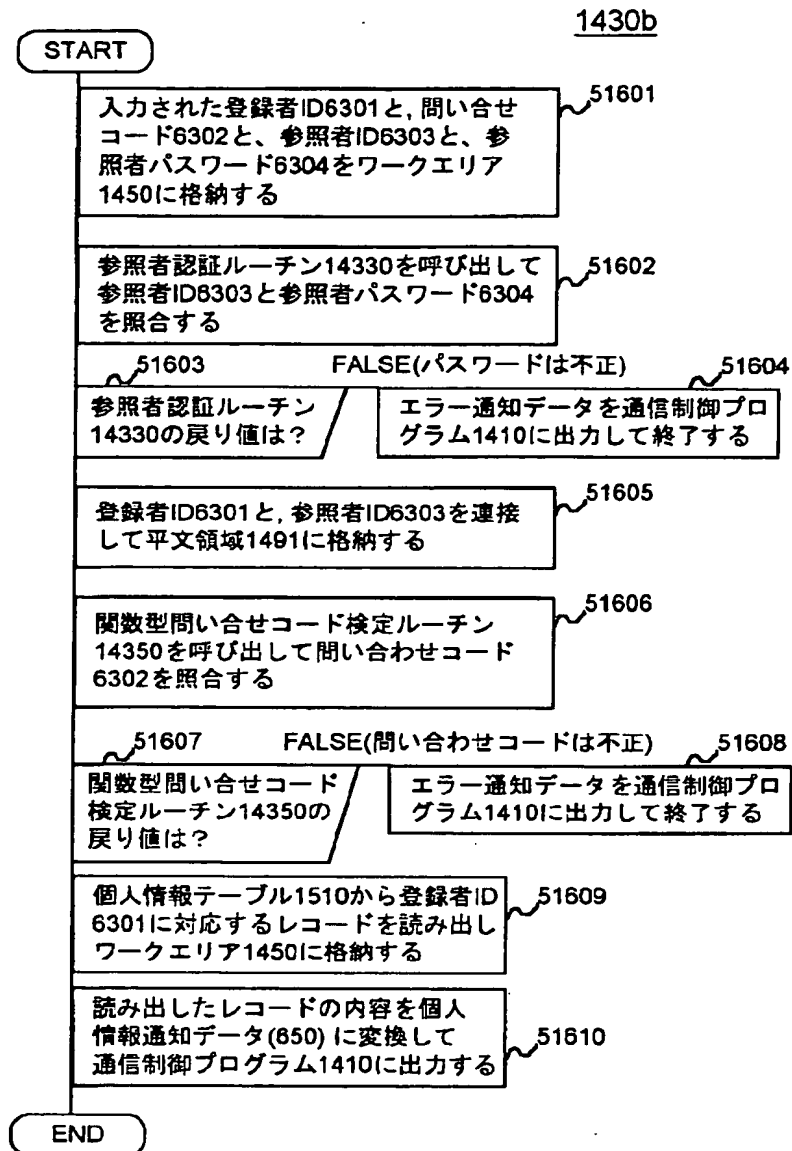
【図 3 5】

図 3 5



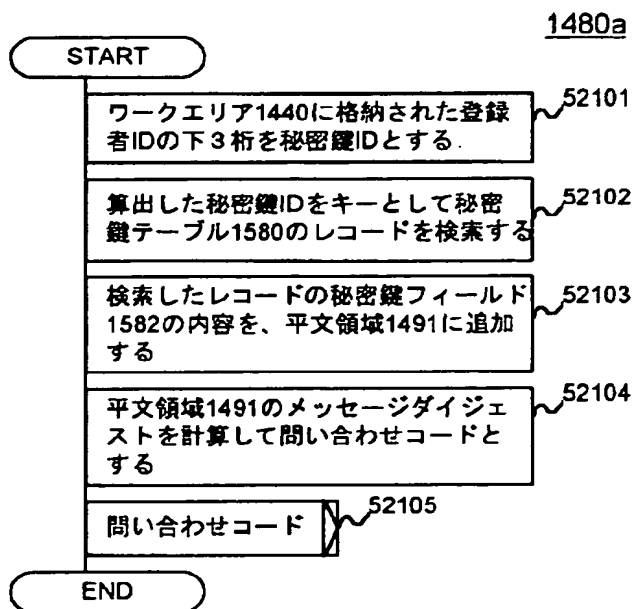
【図36】

図36



【図 4 0】

図 4 0



フロントページの続き

(72)発明者 武田 景

神奈川県川崎市幸区鹿島田890番地 株式  
会社日立製作所情報・通信開発本部内